mobile business

Privacy & Multilateral Security in Mobile Communications
Protecting Identity and Location Information in Mobile Communications

International School on Foundations of Security Analysis and Design (FOSAD)

Bertinoro, 2008-08-25/26

Prof. Dr. Kai Rannenberg
Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt, Germany

fidis

PICOS

Premium*

PRIME

PrimeLife

mobile business

Agenda

- Privacy in a data intensive Information Society
- Identity Management
- Multilateral Security
- Enhancing Privacy via Intermediary Architectures and Choice
- Learnings for Development, Research, Standardisation
- Conclusions & Outlook

Agenda

- Privacy in a data intensive Information Society
  - Mobility and Privacy
  - Mobile Business
  - Mobile Advertising
  - Terminology and Principles
- Identity Management
- Multilateral Security
- Enhancing Privacy via Intermediary Architectures and Choice
- Learnings for Development, Research, Standardisation
- Conclusions & Outlook

Privacy and typical competitors

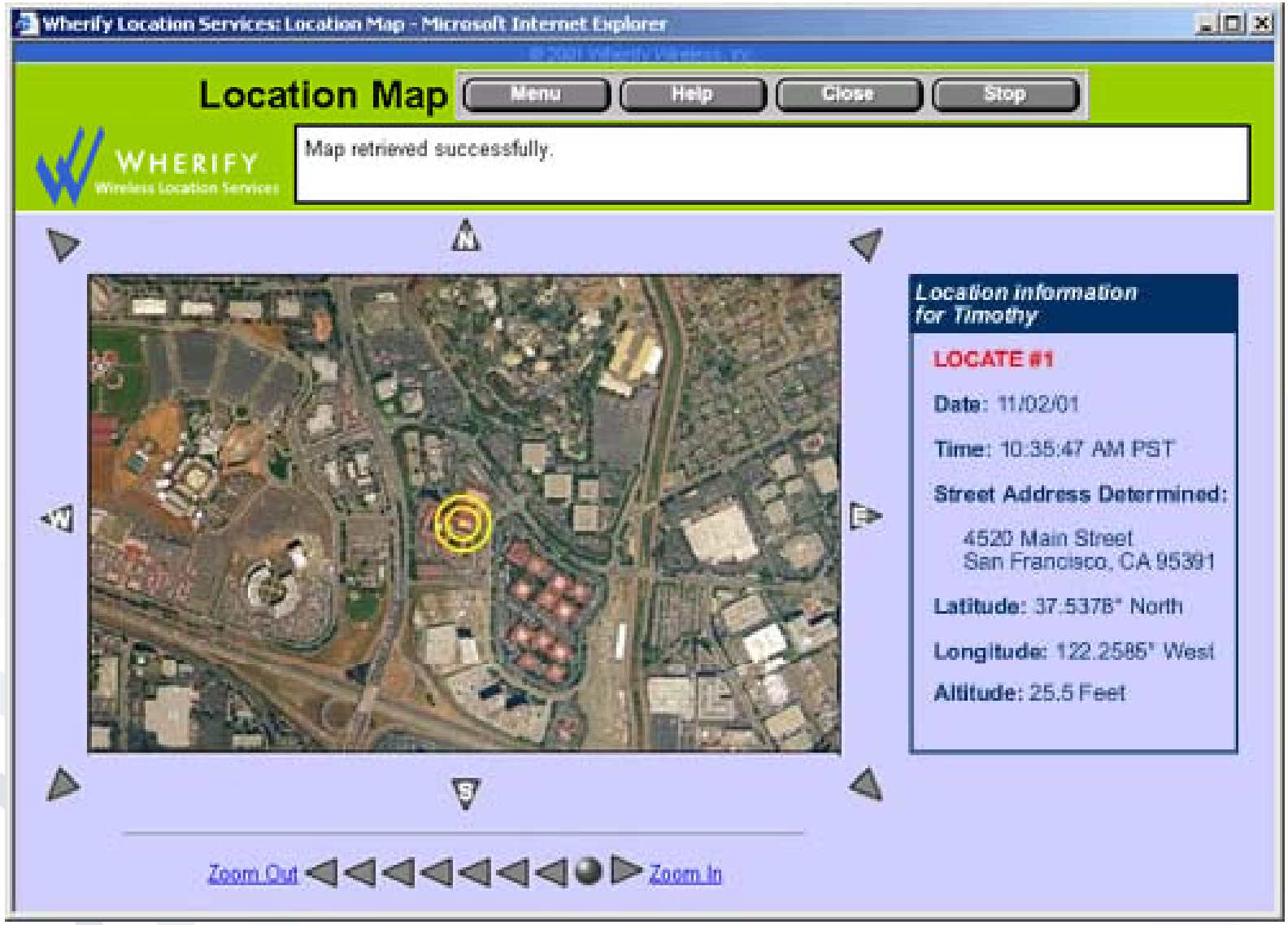
- Data-intensive communication systems and applications
- Other Informatics paradigms
  - Personalisation & User orientation
  - Context awareness
  - Convenience
  - Dependability
  - Security
- Legacy Systems Integration
- Standardisation

Agenda

- Privacy in a data intensive Information Society
  - Mobility and Privacy
  - Mobile Business
  - Mobile Advertising
  - Terminology and Principles
- Identity Management
- Multilateral Security
- Enhancing Privacy via Intermediary Architectures and Choice
- Learnings for Development, Research, Standardisation
- Conclusions & Outlook

mobile business

Child Watch I



Child Watch II

Built-in Pager
Receives and stores up to 10 numeric pages.

Atomic Clock Synchronized
The watch sets itself accurately, no matter what time zone you're in.

Kid-tested. Kid-tough
Rugged, lightweight and adjustable locator is water-resistant and cut-resistant.

Request 911
Wearer presses two outer buttons for 3 seconds to initiate a 911 emergency response; Subscriber may deactivate this feature.

Key Fob
Manually locks and unlocks locator.

Lock Button
Press to automatically lock locator.

GPS Technology
Integrated GPS and digital wireless technologies pinpoint the wearer's location.

Patented SafetyLock™
Prevents unwanted removal; activate manually or remotely.

Child Watch III

- Children have GSM-GPS system on wrist.
- Price: US$ 199,99 (399,99)
- Example Service Plan: „Liberty“
  - US$ 19,95 (25) /Month
  - 4 free 911 alert calls, any further call US$ 15
  - 20 free localisations, any more US$ 0,95

www.wherifywireless.com

WHERIFY

With a Wherifone you can quickly,
Locate, Communicate.

WHERIFONE
FOR THE...

CHILD

SENIOR

EMPLOYEE

WHERIFONE

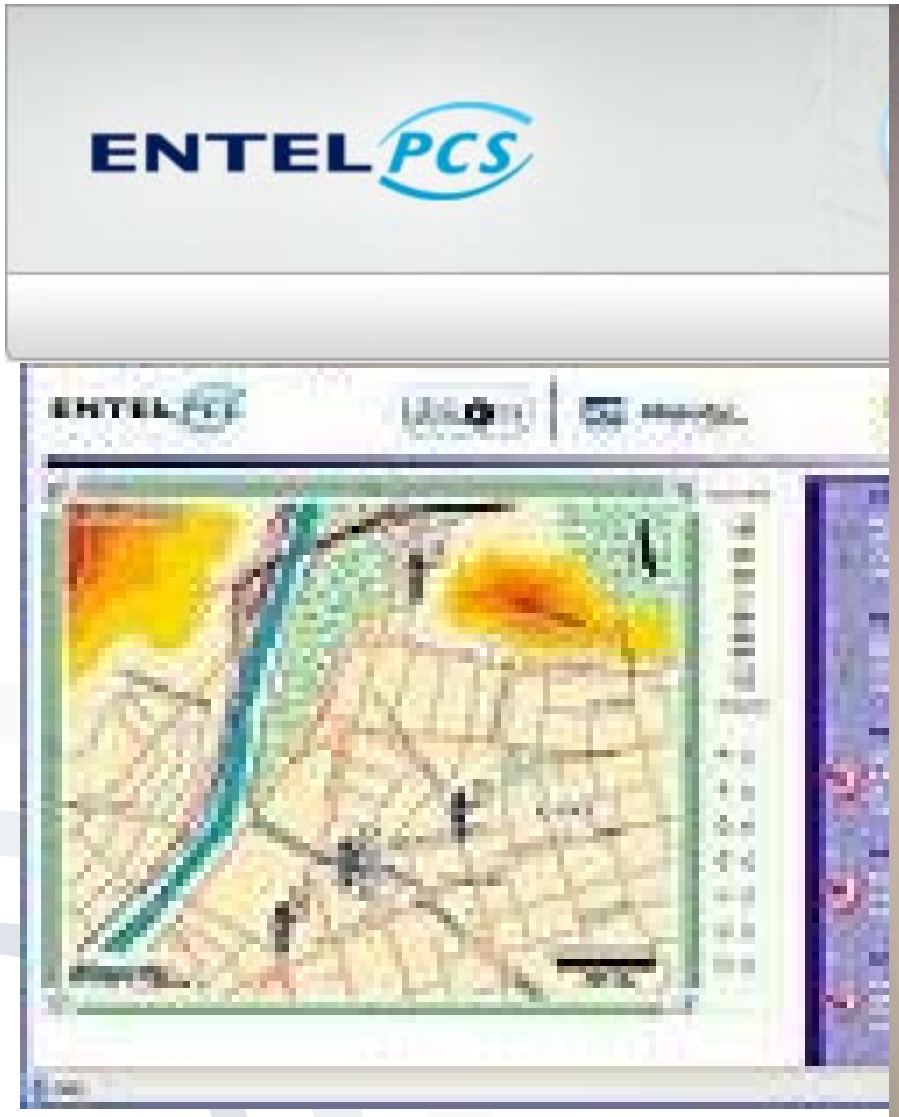
Whether used as a "First Phone" for pre-teens, as a "Companion Phone" for seniors or special needs family members, or as a Mobile "Work Phone," the Wherifone GPS locator phone provides affordable peace-of-mind to the modern mobile family and the business on the move.

View the Wherifone Features and Scenarios to see how Wherifone fits your lifestyle.

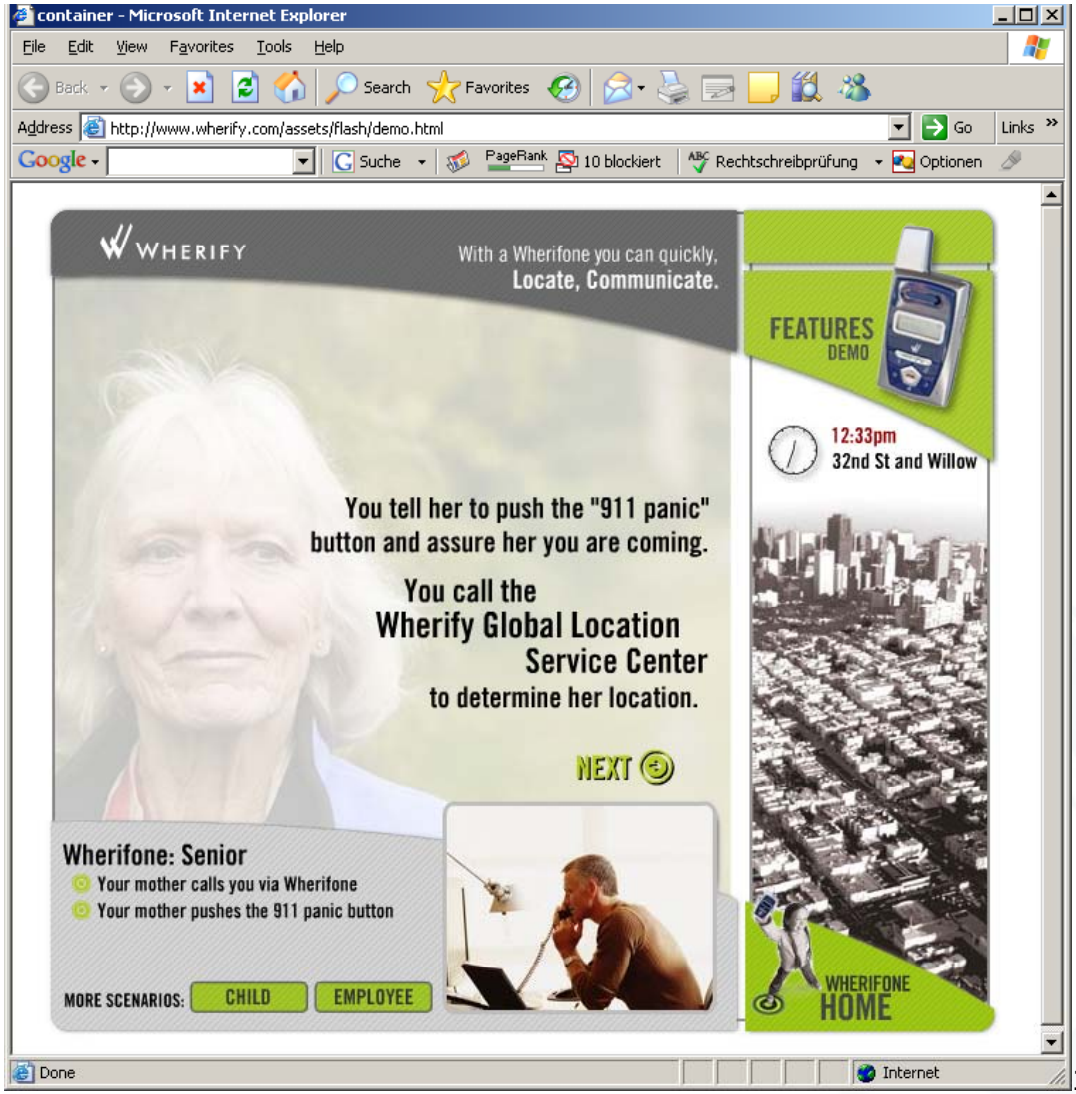
FEATURES
DEMO

mobile business

… in Chile marketed by a mobile operator (Entel PCS)

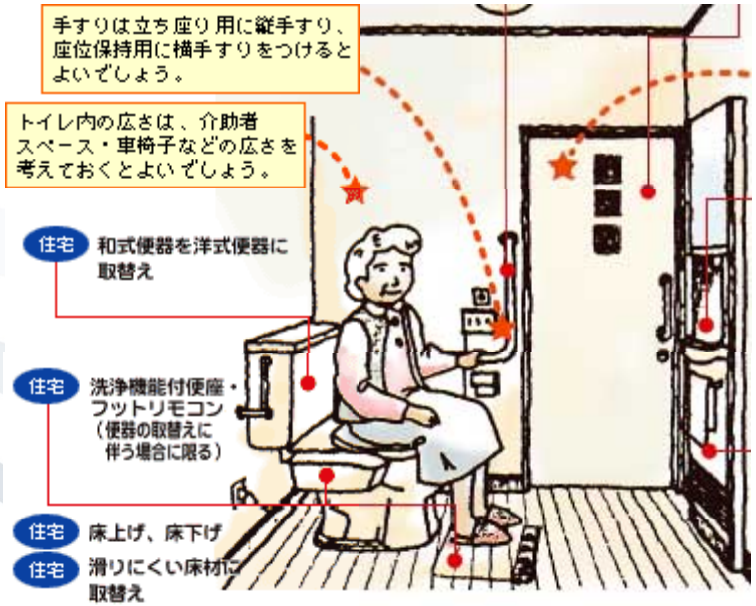


For Senior Citizens also …



The networked washlet

- … and in Japan, Matsushita has demonstrated a health-monitoring toilet that can analyze your stool and send the information online to your doctor. [www.asiaweek.com/asiaweek/technology/article/0,8707,130495,00.html, 2001-06-22]
- “ … sensors detect seven abnormal behavior patterns of the elderly in their living quarters and three abnormal patterns in the toilet area. Any abnormality that is sensed is automatically transmitted to the PHS terminals or pagers of the nursing staff. The care monitor system that uses these sensors will help provide safe and high quality nursing service.” [www.mew.co.jp/e-tecrepo/73e/main02.html]



[Hitachi, Matsuhita Electric Works Limited, Panasonic, Toto]

Networked health care and monitoring system

Abstract:A networked health care and monitoring system (10) capable of **providing an updated reliable vital information** on the health condition of individuals and adapted to support home health care and maintenance. The system includes testing and measuring instruments (39; 43; 46; 49; 56) associated with certain household appliances such as a toilet system (12) and adapted to monitor the vital information passively in response to the use thereof in connection with routine living activities of the individuals. The system may further include control devices (39; 46; 49; 56) associated with certain household appliances, such as an ergometer (15), having health care and maintenance functions and adapted to control the appliances based on the vital information monitored by the testing and measuring instruments in the system. In one embodiment wherein the system is arranged in the centralized network configuration, the testing and measuring instruments and the control devices are connected via a local area network with a data controller (20) wherein all the vital information obtained in the system is stored. Instruments and devices (39; 43; 46; 49; 56) are **permitted to access the controller through the network** to retrieve necessary vital information therefrom. In another embodiment arranged in the distributed network configuration, the vital information obtained by respective measuring instruments is stored therein and is furnished upon request to the other appliances.

[United States Patent 5410471, www.freepatentsonline.com/5410471.html]

mobile business

Cars are becoming networked (mobile) Computers

- Car anti-theft Control
  - Checks car for impact
  - „Calls“ owner in case of problems
  - Immobilizes car in suspicious situations
  - Tracks stolen cars
- Road Tolling
  - Number plates get registered.
  - Cars can get tracked.

➢ Who decides what?

➢ User empowerment is crucial.

What can one see from these examples?

- ICT infrastructures, applications and services
  - get ever more powerful
  - get closer to people
  - do what used to be ”human privileges”
- Advanced applications depend on
  - Networks & Devices
  - More and more context information
  - User Trust and Confidence

➢ Privacy is
  ➢ important for trust and confidence
  ➢ a moving target, as IT applications are moving so fast.

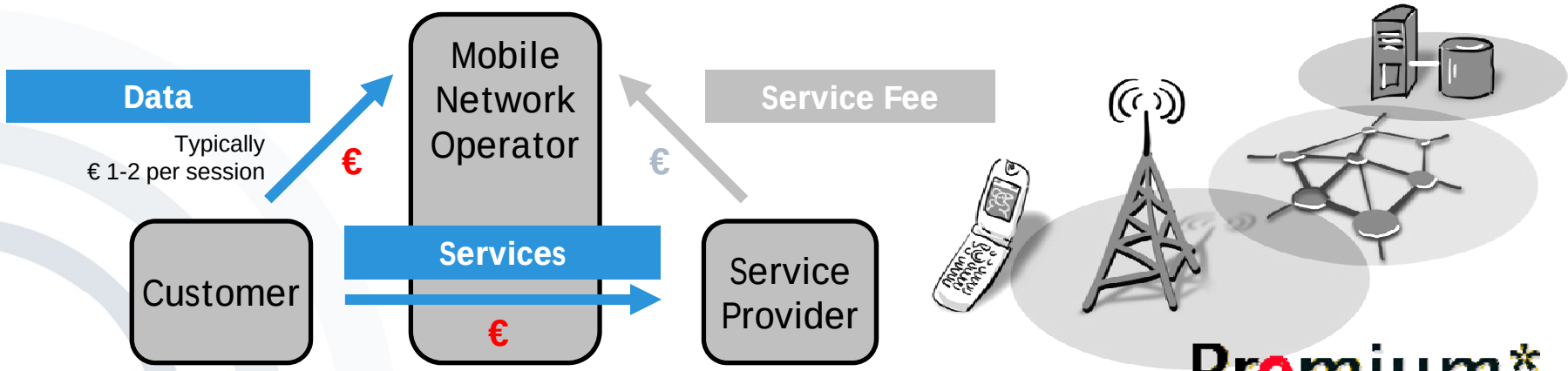
➢ There is an even more commercial side to this including Identity Management

Agenda

- Privacy in a data intensive Information Society
  - Mobility and Privacy
  - Mobile Business
  - Mobile Advertising
  - Terminology and Principles
- Identity Management
- Multilateral Security
- Enhancing Privacy via Intermediary Architectures and Choice
- Learnings for Development, Research, Standardisation
- Conclusions & Outlook

Classic approach for M-Commerce business models

- Mobile Network Operators provide their customers with **mobile portals** as access concept for mobile services.
- Revenue models with two revenue sources:
  - **Mobile Data** (Internet Service Providing)
  - **M-Commerce Services** (by Service Providers)
- Only services providing **immediate value** for customers.
- Services with **primary value for Service Providers** are currently not feasible (Advertising, Customer Loyalty Programs etc.).



Some trends in the Mobile Data Communications Market

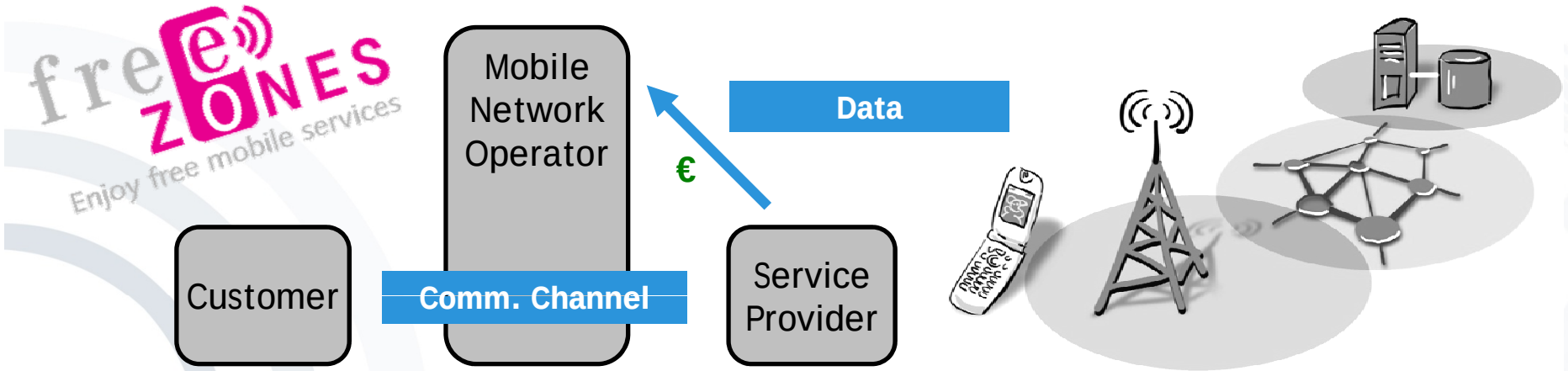
- Number of mobile Internet users increasing significantly
  - Availability of “quasi” flat rates
  - Improved usability of mobile devices (eg. iPhone)
  - Constantly increase of number of mobile services

- Increasing competition for the attention of mobile customers (IP, Device, Telco)
  - Google develops of mobile operating system Android
  - Mobile Portal Yahoo! oneSearch
  - MVNO Blyk offers free mobile voice services in exchange for receiving SMS-based advertisements
  - Mobile advertising platform AdMob.com delivers more than 5 Mill. ads per month
  - …

A new Value Proposition is developing

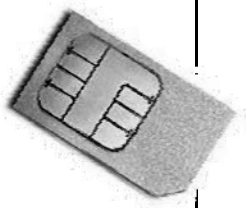
- **Potential:** Mobile network operators have a customer relation with e.g. more than 85% of the German population!
- **Offering:** Mobile network operators are providing service providers with a communication channel to potential customers.
- **Motivation:** Service providers gain higher, mobile initiated revenues in their business.
- **Objective:** Eliminating data costs for customers while making them marketing costs for service providers.

Premium*



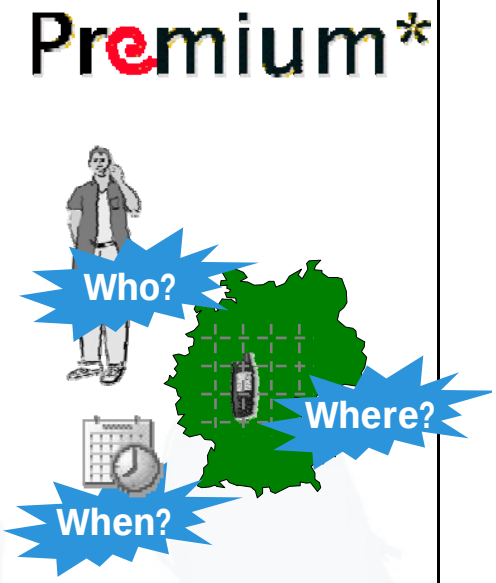
Mobile Network Operators as Identity Managers

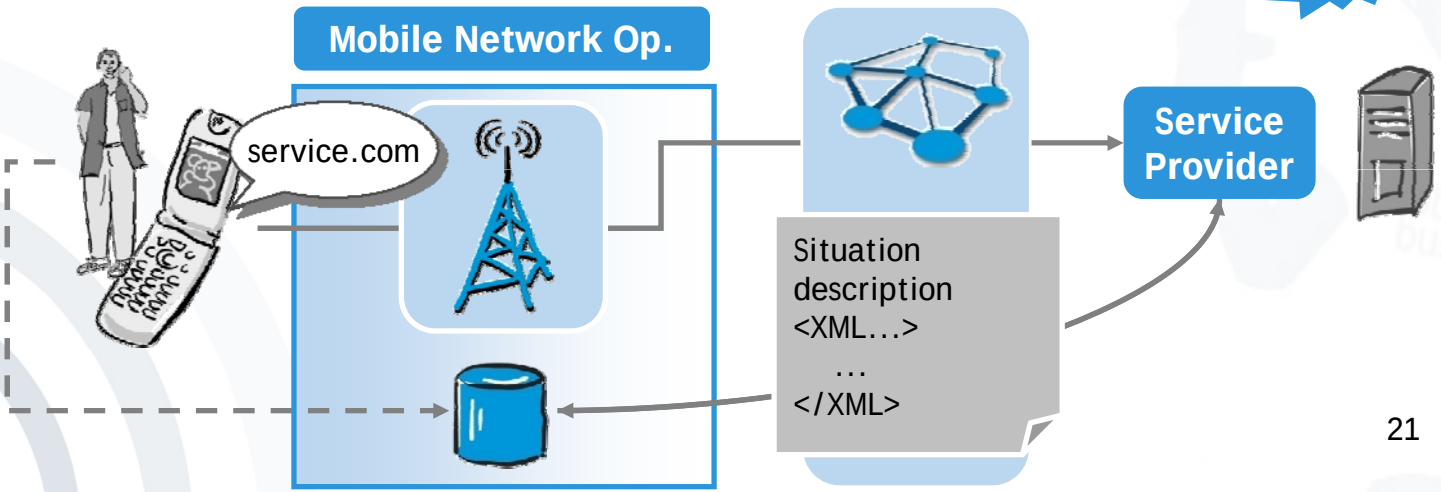
- Mobile Network Operators already manage identities
  - SIM = **Subscriber Identity Module**
  - **2.9 billion GSM (SIM)** subscriptions (4Q 2007)
  - More countries with SIM infrastructure (220, 4Q 2007) than McDonalds (118, 05.2008) and UN-members (192, 05.2008).
- **Relevance of identity management** grows
  - **Due to legal conditions** of location based services and the processing of personal data
  - "Who is allowed to localise whom when and where?"
- **Trusted party and intermediary role**
  - offers telecommunications providers new opportunities.
  - solves industry problems: customised offers minimise churn and allow for price and tariff discrimination.



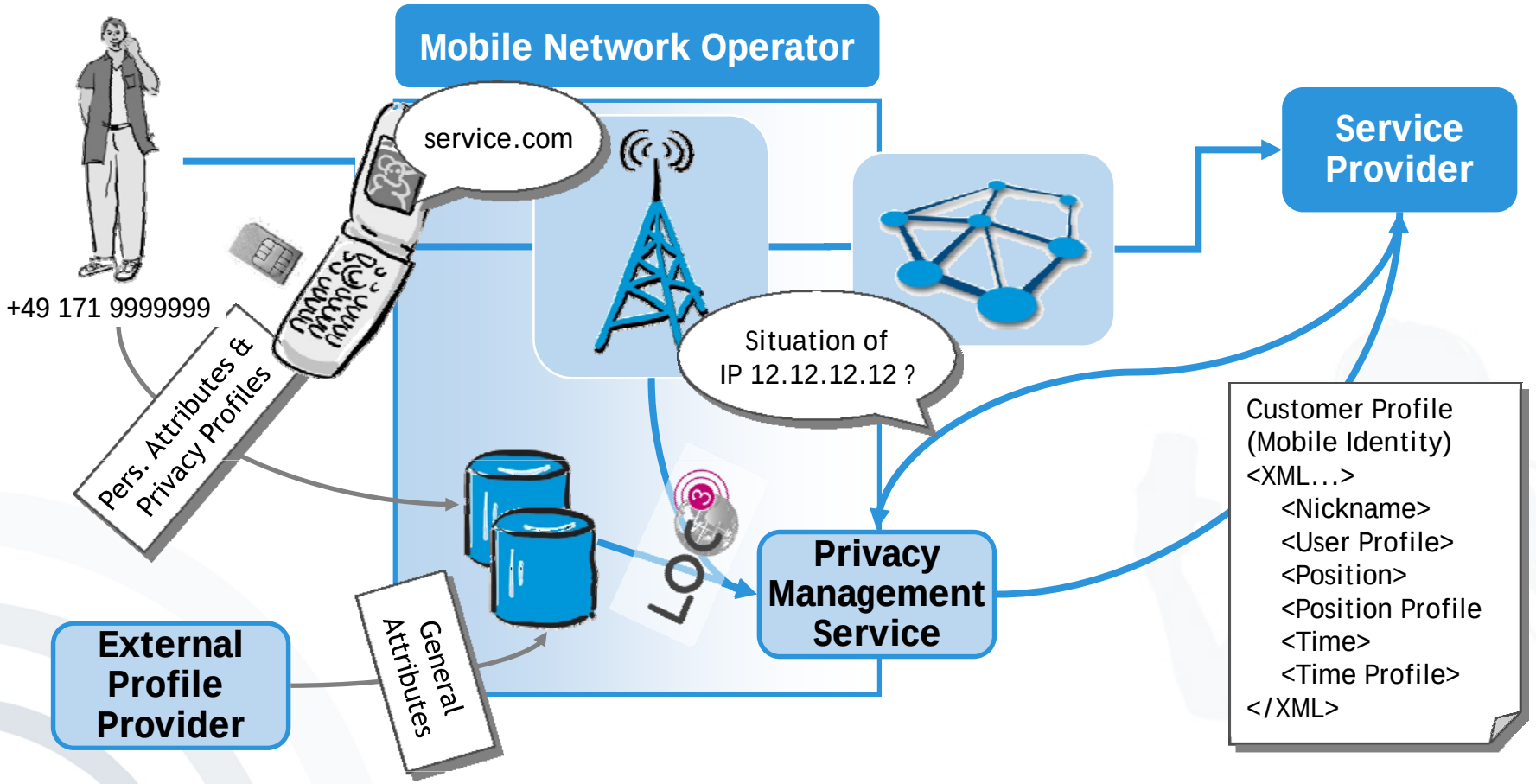
Mobile Identity and Situation Dependency

- Mobile network allows determination of
  - **identity** and
  - **position** of the user as well as
  - **time** of usage.
- Information can be extended by using databases and is delivered as **situation description** to service providers.
- Sample result: „Customer is 25 years old, student, in downtown Bologna, on holiday, …“

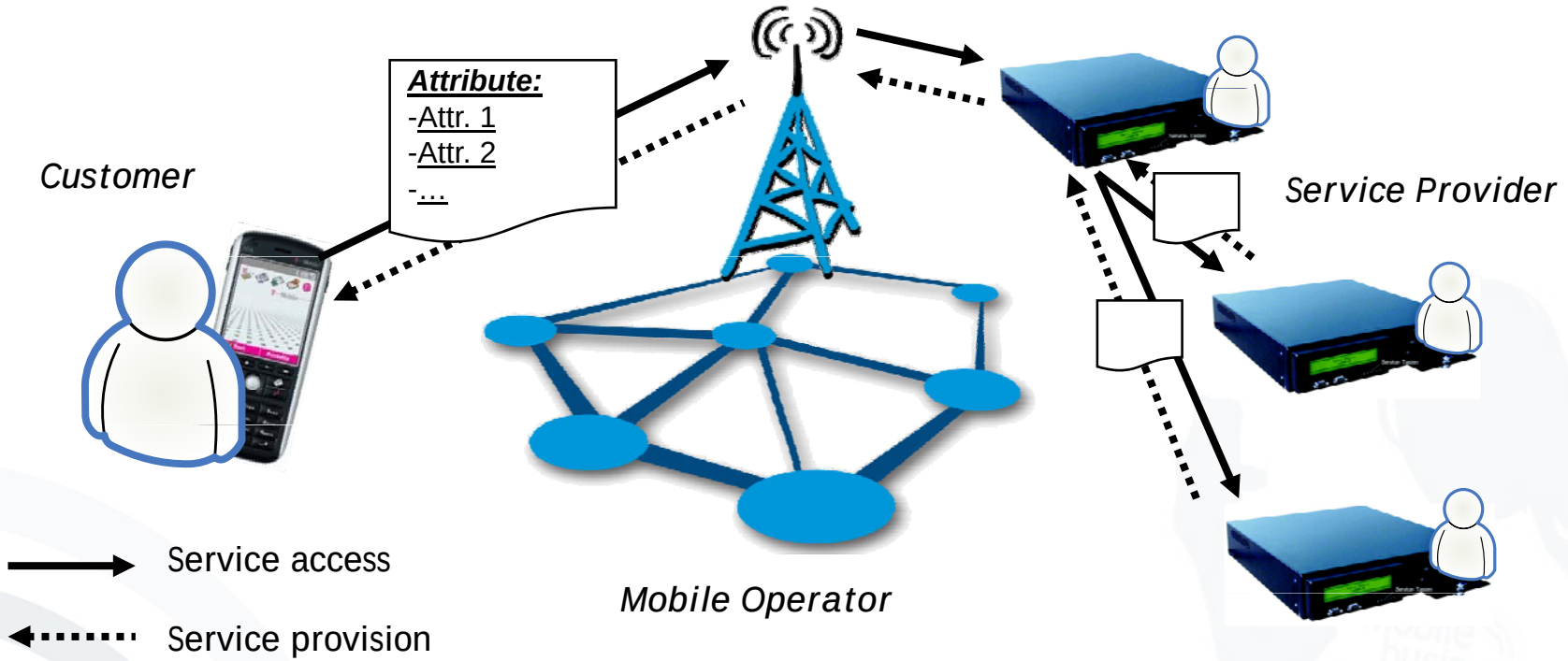




Mobile (Digital) Identity



User controlled transfer of Attributes

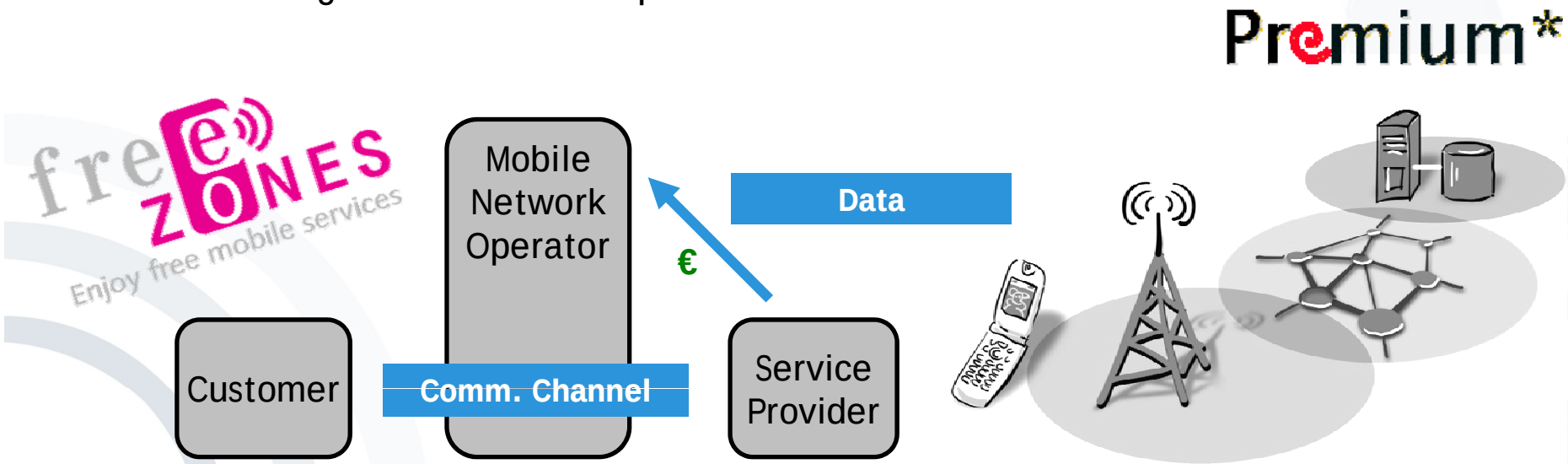


Agenda

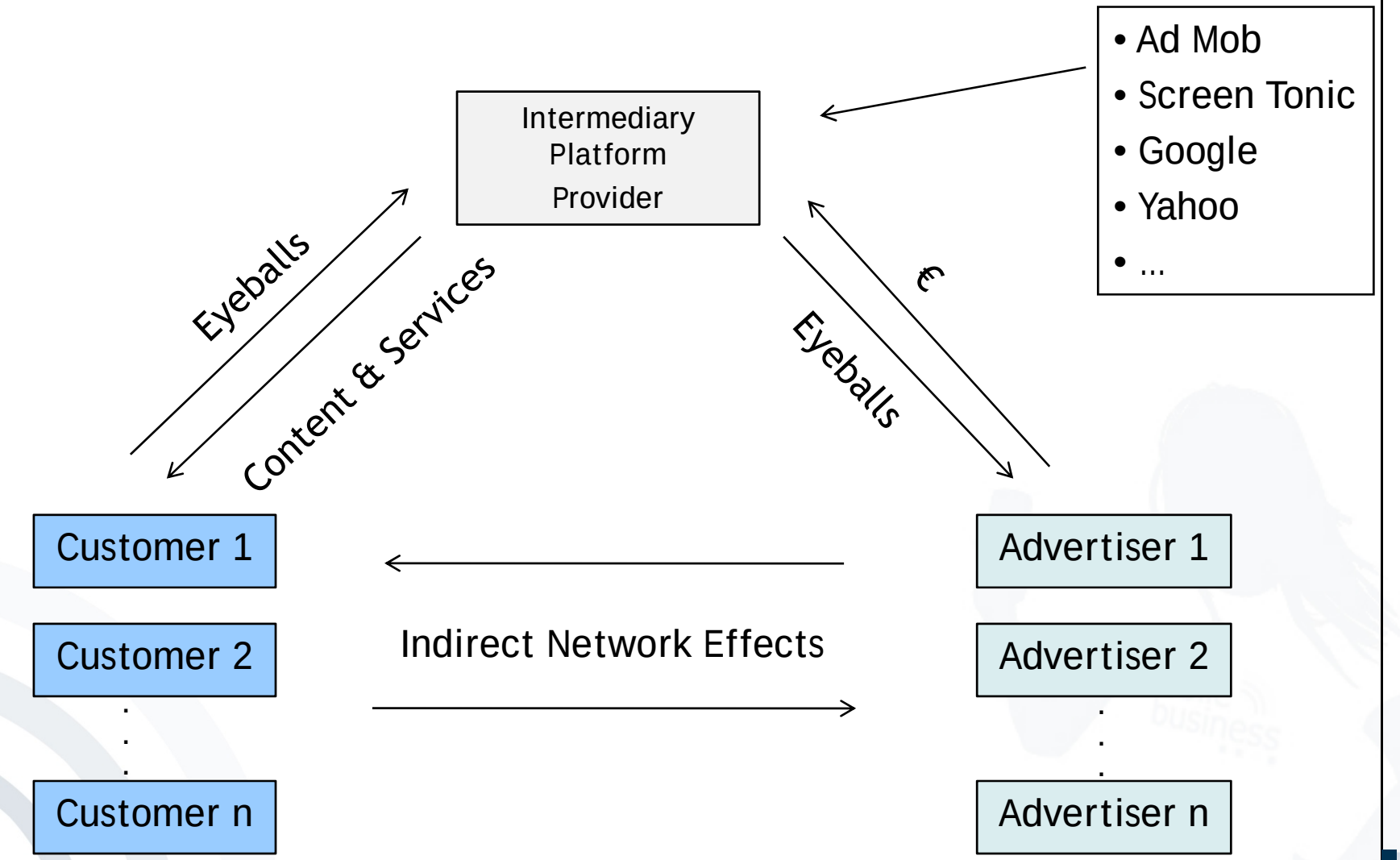
- Privacy in a data intensive Information Society
  - Mobility and Privacy
  - Mobile Business
  - Mobile Advertising
  - Terminology and Principles
- Identity Management
- Multilateral Security
- Enhancing Privacy via Intermediary Architectures and Choice
- Learnings for Development, Research, Standardisation
- Conclusions & Outlook

Advertisement sponsored mobile communication

- **Potential:** Mobile network operators have a customer relation with almost the complete population!
- **Offering:** Mobile network operators are providing service providers with a communication channel to potential customers establishing a 2-sided market.
- **Motivation:** Service providers gain higher, mobile initiated revenues in their business.
- **Objective:** Eliminating data costs for customers while making them marketing costs for service providers.

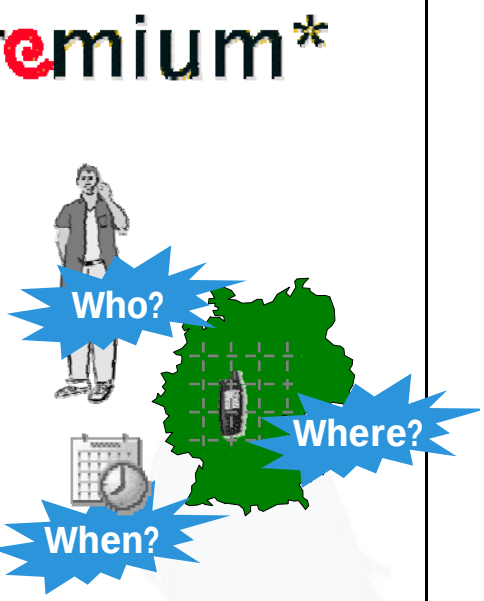


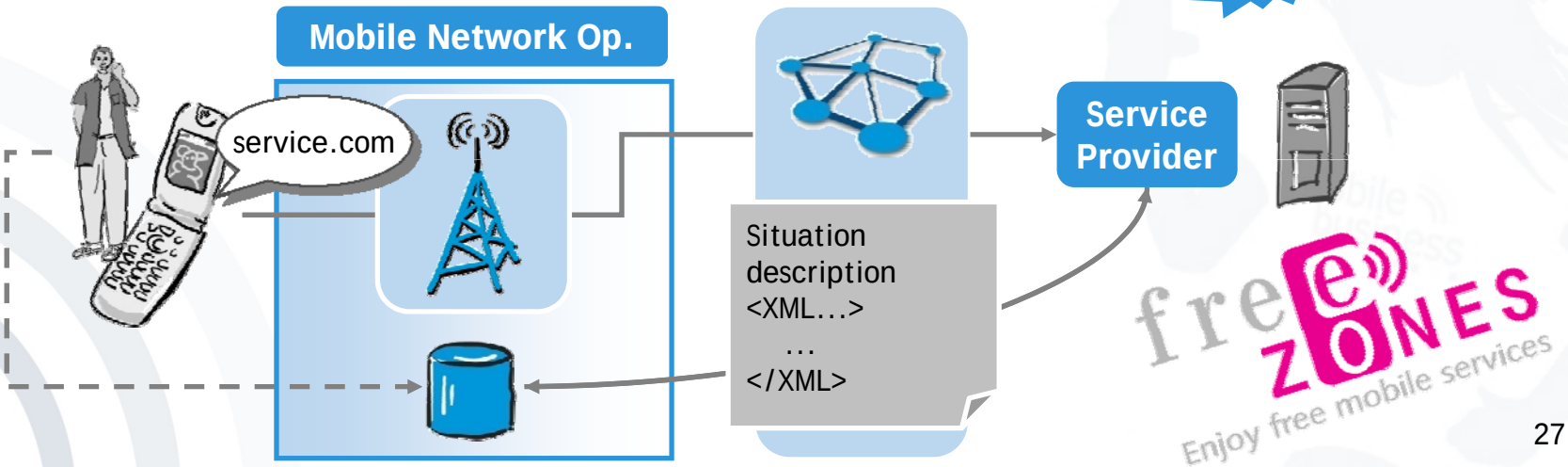
Two-sided Mobile Communications Media/Marketing Market



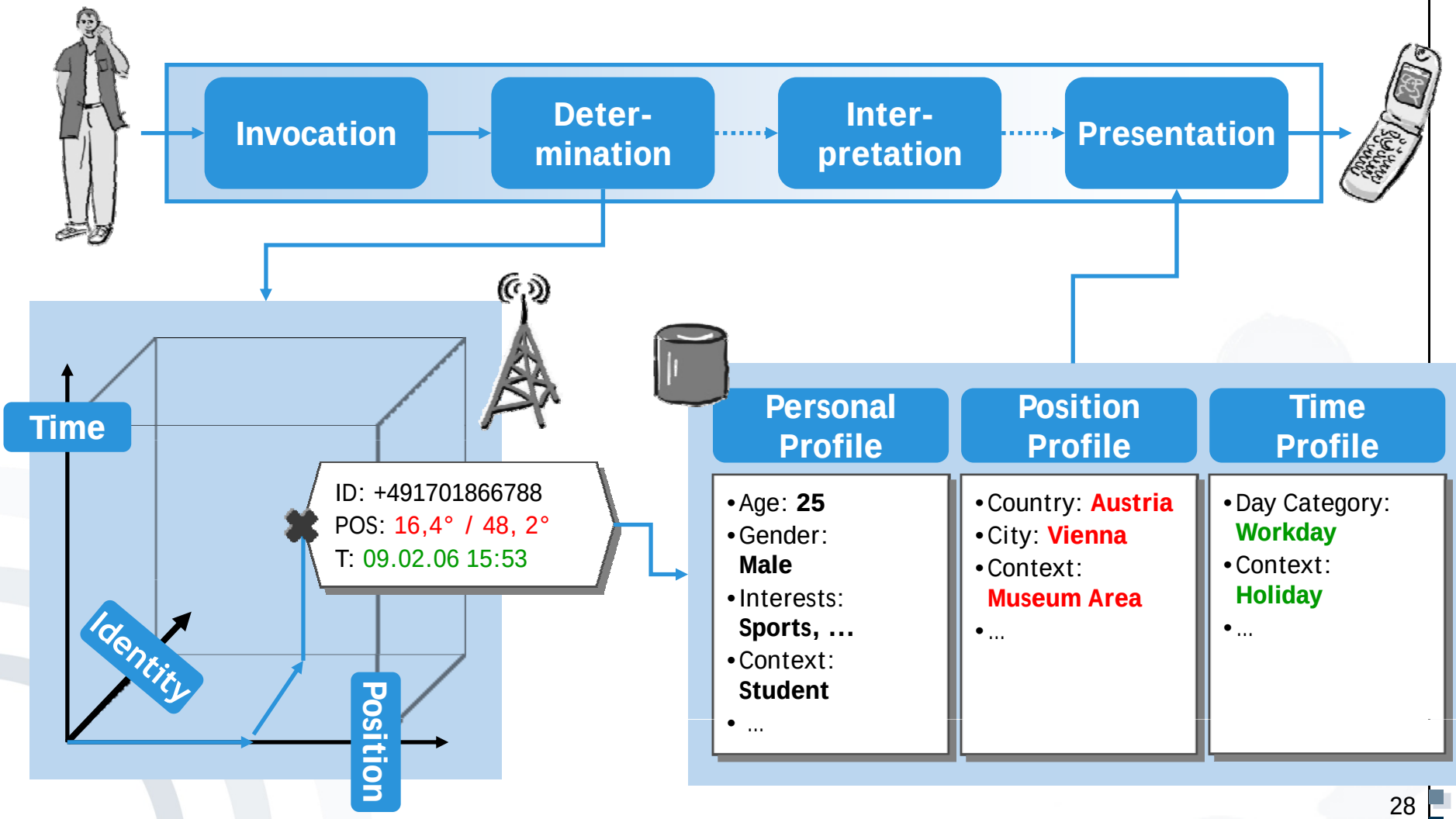
Situation & Profile based mobile Advertising

- Mobile network allows determination of
  - **identity** and
  - **position** of the user as well as
  - **time** of usage.
- Information can be extended by using databases and is delivered as **situation description** to service providers, e.g. for **advertisement sponsored communication**
- Sample result: „Customer is 25 years old, student, in downtown Bologna, on holiday, …“



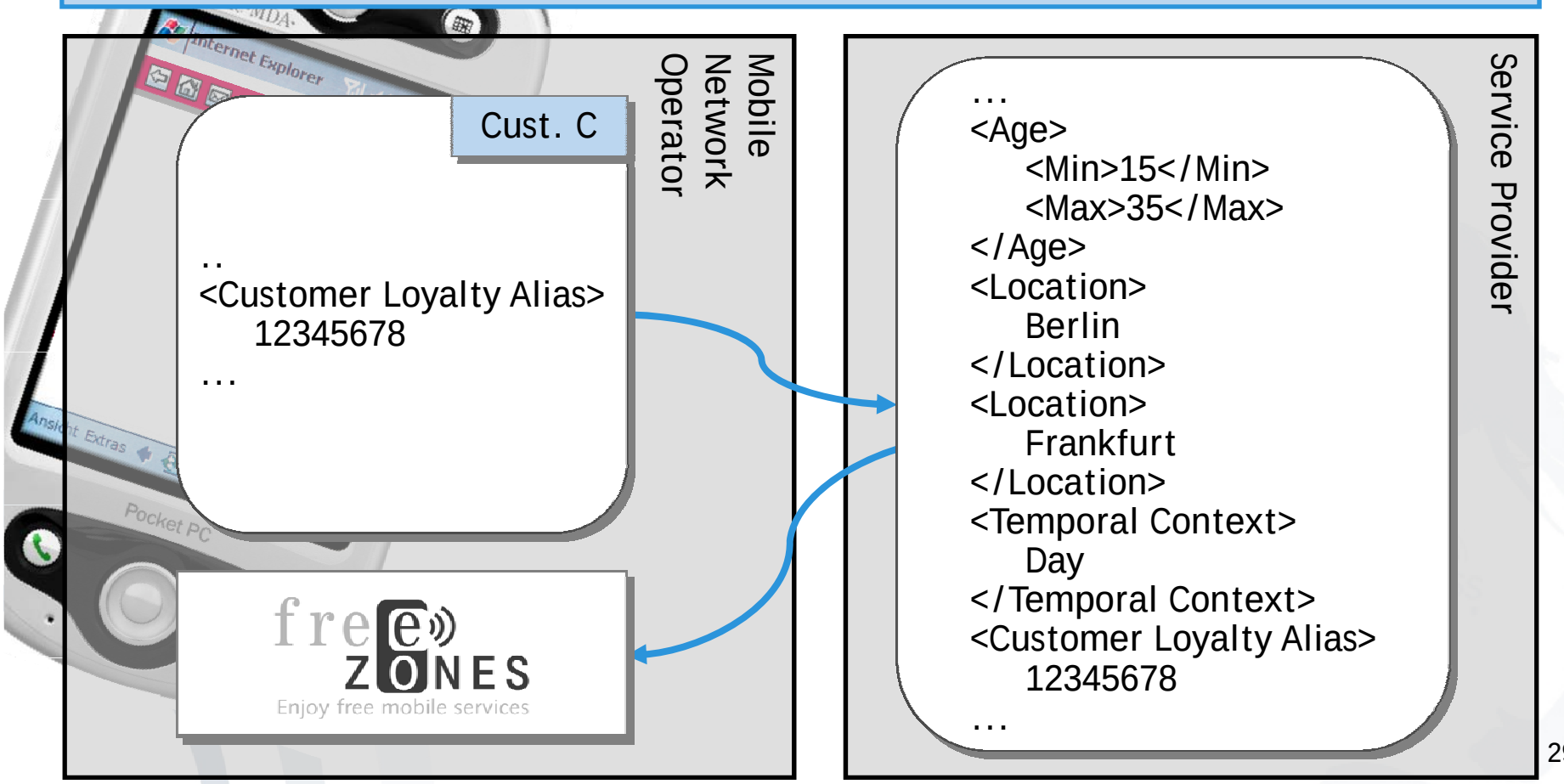


The "Situation Process"

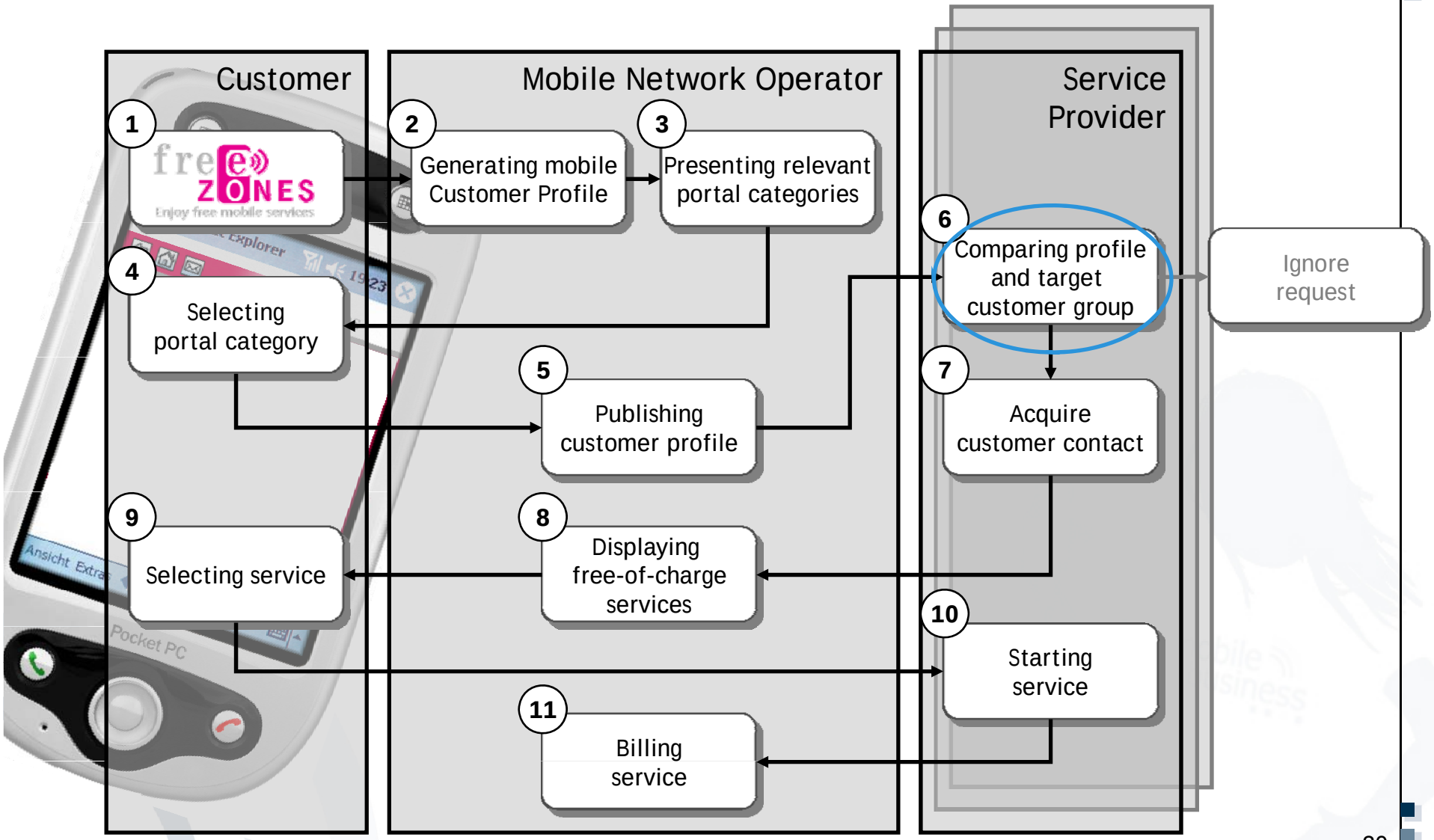


Comparing Profile and Target Customer Group

- **Customer:** Selects portal category *Food & Meals*
- **Mobile Network Operator:** Generates customer profile and transfers it to relevant service providers (e. g. McDonalds, Coca-Cola etc.)
- **Service Provider (example):** McDonalds with branches in Berlin and Frankfurt

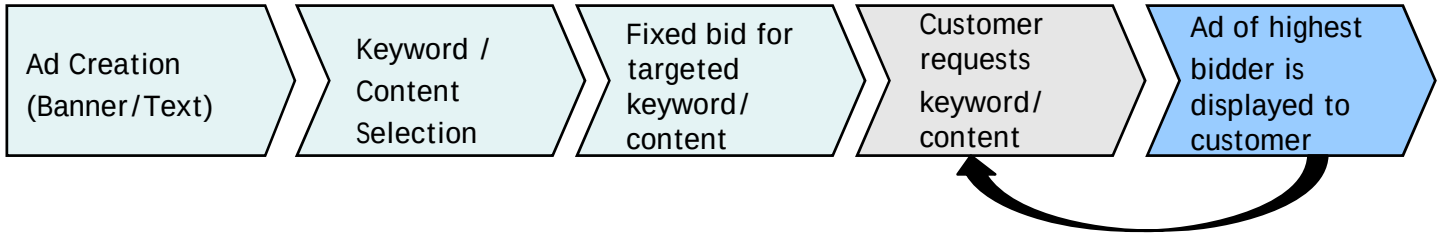


Situation & Profile based mobile Advertising – Process View

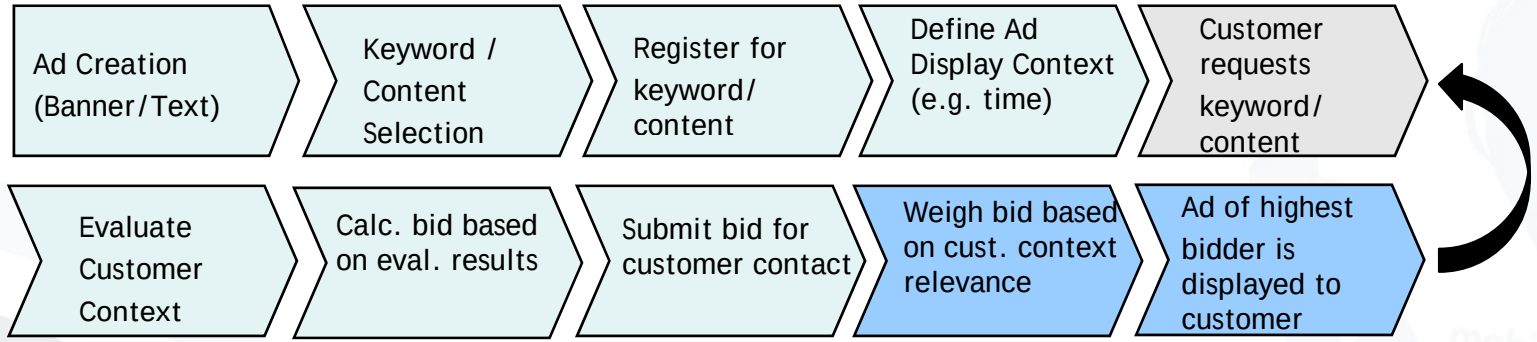


“Traditional” vs. Context-sensitive Mobile Advertising

“Traditional” Mobile Advertising (cp. Yahoo or Google)



Context-sensitive Mobile Advertising



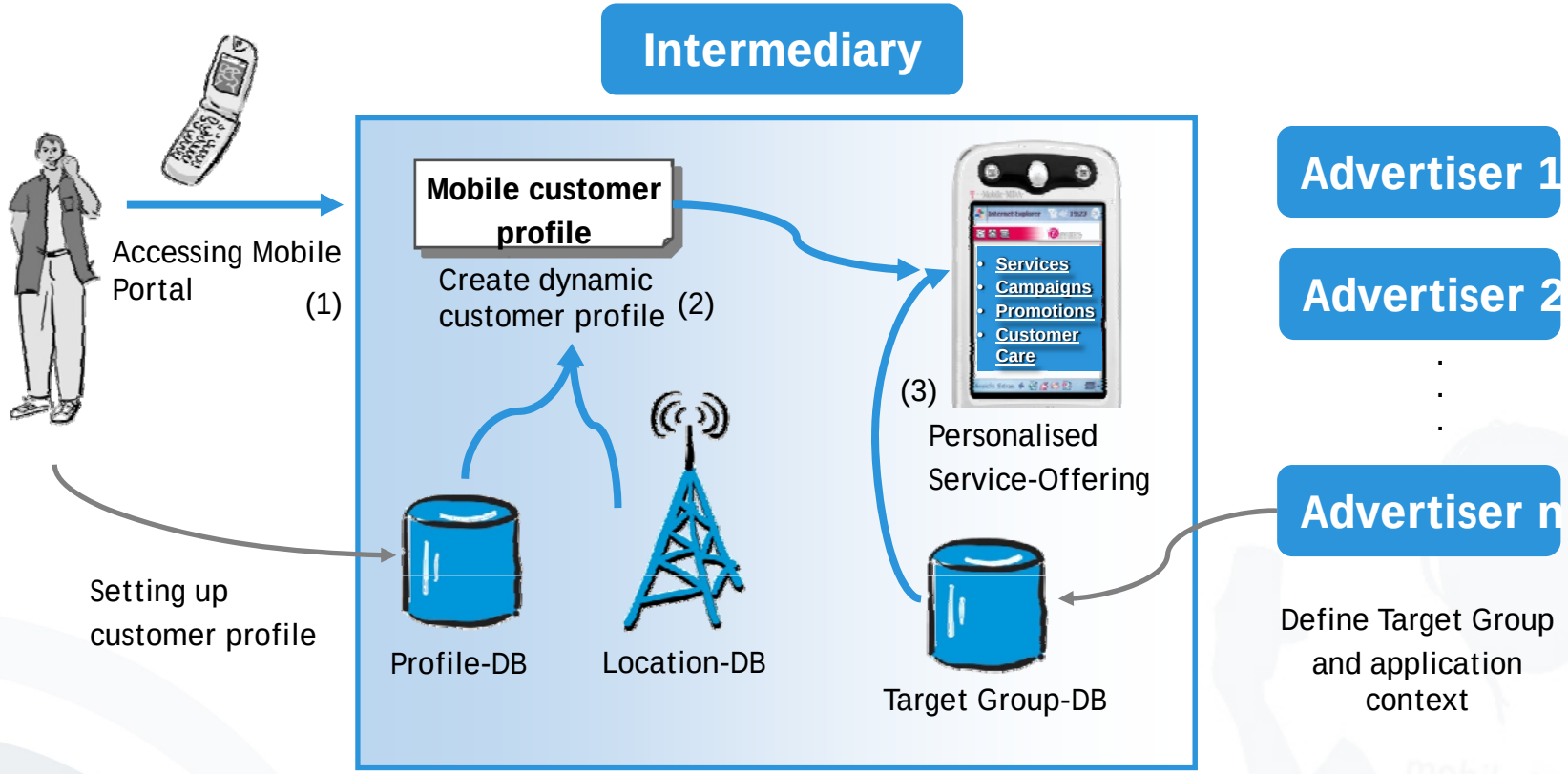
Customer

Advertiser

Intermediary

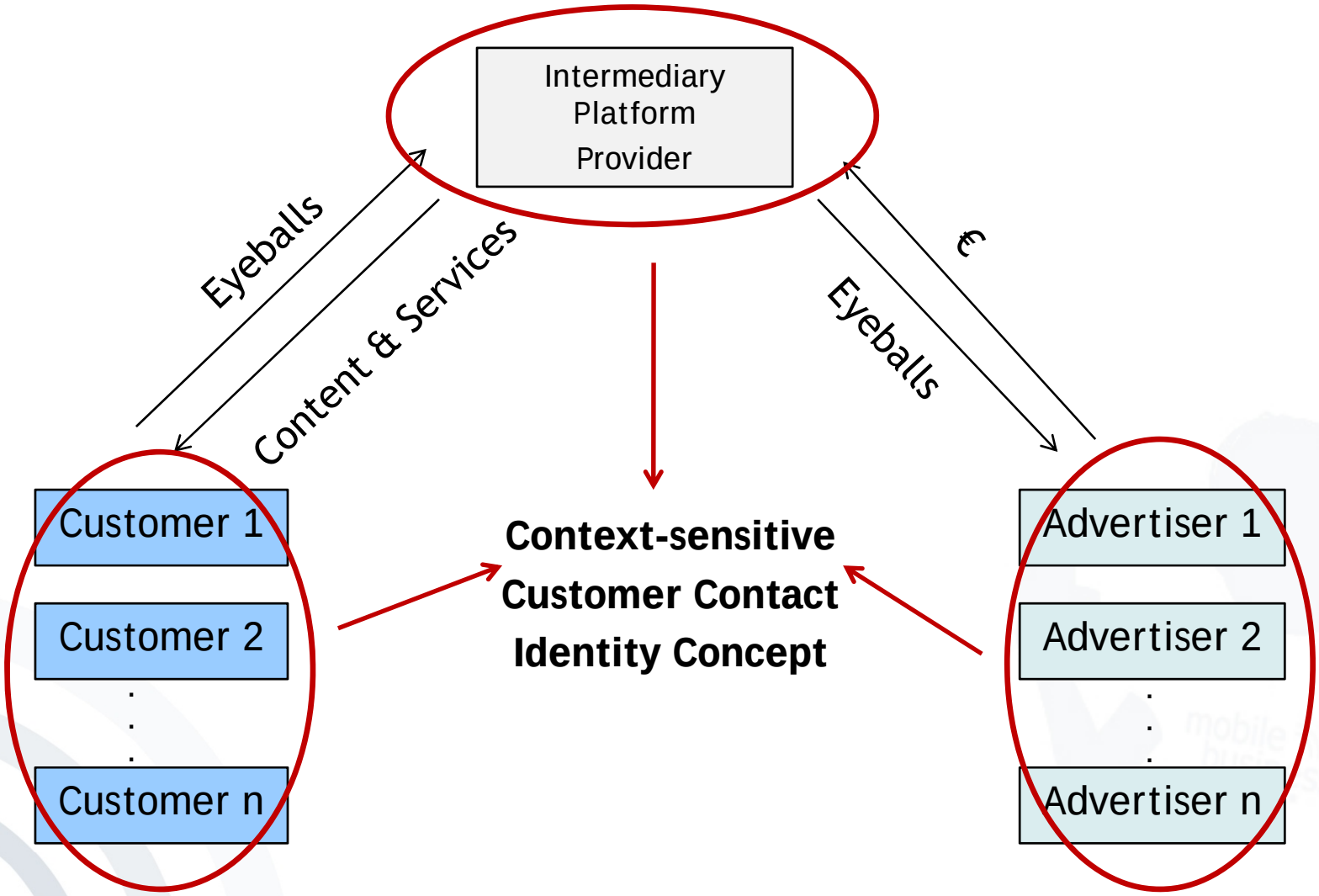
[Andreas Albers]

Context-sensitive Mobile Marketing using a Mobile Portal



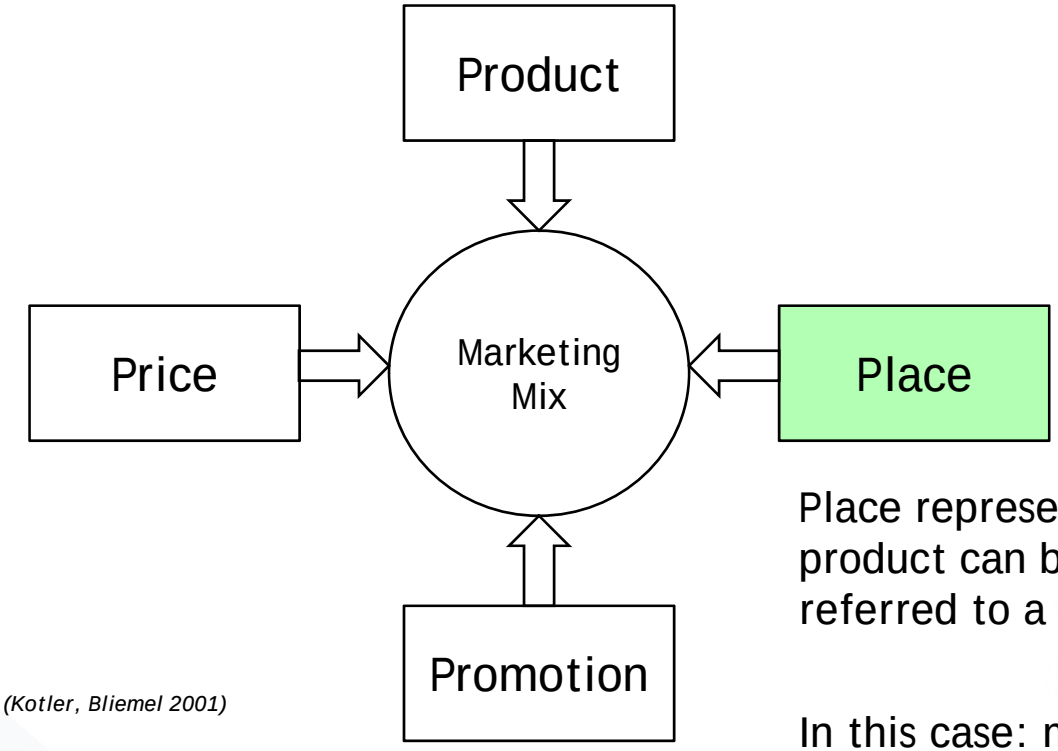
- Sample scenario: Restaurant Finder, returning only restaurants in close distance with appropriate opening hours and matching a user's general interest profile.

Impact of Context Information on the two-sided market



- Common understanding between market players required about underlying identity concept of customer contact

Recommender Systems for Marketing/Advertising



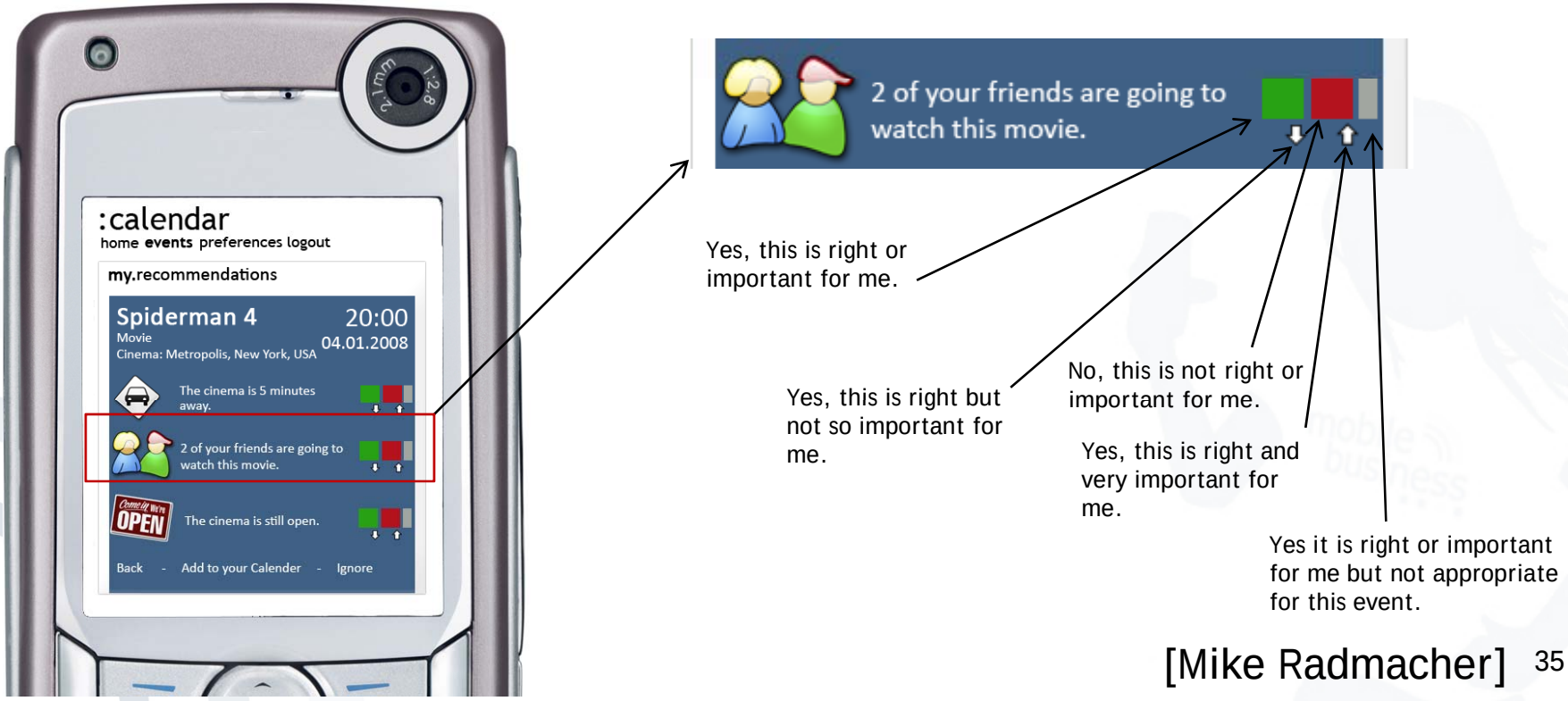
(Kotler, Bliemel 2001)

Place represents the location where a product can be purchased. It is referred to a distribution channel.

In this case: mobile recommendations are used as distribution channel in a virtual shop, the place where products can be purchased.

Recommender Systems
Transparency and Feedback

- Explanation / Questioning of Recommendations:
  - Users tend to place more trust into understandable recommendations.
  - Recommendations improve via user feedback.



[Mike Radmacher]

Agenda

- Privacy in a data intensive Information Society
  - Mobility and Privacy
  - Mobile Business
  - Mobile Advertising
  - Terminology and Principles
- Identity Management
- Multilateral Security
- Enhancing Privacy via Intermediary Architectures and Choice
- Learnings for Development, Research, Standardisation
- Conclusions & Outlook

Data Protection and Privacy

- Both terms are related but not synonymous and have many definitions.
- 2 popular ones:
  - Data protection is the protection from harmful and unsolicited usage of data linked to the personal sphere of a person.
  - Privacy is the right to be let alone. [WaBr 1890]
- More work needed on a complete understanding of privacy
- Nevertheless the topic is important, as one can see from related incidents and activities to address the issue.

The origin of data protection?

- The term “Privacy” (‘the right to be let alone’) originates from [WaBr1890].
- Data protection in Germany (“Datenschutz”) originates from concerns over too much information und power in the hands of large (governmental” institutions (“Big Brother”).
- Nowadays Data protection and Privacy in Germany are based on the right of informational self determination derived from the constitution in the “Volkszählungsurteil“ [BVG 1983]).
- Germany has one of the most advanced infrastructures for Privacy but still no established German language term for Privacy beyond the (misleading) “Datenschutz”.
- Some (more or less established) related terms are:
  - Privatheit
  - Privatsphäre
  - Schutz der Privatsphäre

9 Principles of EU Privacy Law I

1. **Intention and notification:** The processing of personal data must be reported in advance to a Data Protection Authority.
2. **Transparency:** The person involved must be able to see who is processing her data for what purpose.
3. **Finality principle:** Personal data may only be collected and processed for specific, explicit and legitimate purposes.
4. **Legitimate grounds of processing:** The processing of personal data must be based on a foundation referred to in legislation, such as permission, agreement, and such.
5. **Quality:** Personal data must be as correct and as accurate as possible

[BlaBorOlk2003]

9 Principles of EU Privacy Law II

6. **Data subject's rights:** The parties involved have the right to take cognisance of and to update their data as well as the right to raise objections.
7. **Processing by a processor:** This rule states that, with the transfer of personal data to a processor, the rights of the data subject remain unaffected and that all restrictions equally apply to the processor.
8. **Security:** A controller must take all meaningful and possible measures for guarding the personal data.
9. **Transfer of personal data outside the EU:** The traffic of personal data is permitted only if that country offers adequate protection.

[BlaBorOlk2003]

Law alone is not sufficient

- The increased usage of IT systems and networks leads to
  - huge amounts of data
  - easily searchable data
  - automatic analysis,
  - and knowledge extraction
- Data protection / Privacy law alone not sufficient
  - Not all processing can be controlled (e.g. every network node).
  - Deliberate breaking and bending of law (different legislations on the internet)
  - Economic pressure can force customers to give consent to almost any kind of 'privacy' policy (e.g. selling privacy for "peanuts").
- Slow pace of privacy self-regulation in the US, Focus on self-help
  - Self regulation by sustaining user ignorance
  - Enforcing norms may violate anti-trust.
  - Being a good actor (e.g. by exposing privacy practices) increases liability.
  - Legal compliance and related business processes (deemed) expensive

[Reagle1998, SelfReg1999, Bell2001, Hoofnagle2005]

⇨ Technical Privacy Protection
⇨ Standardisation

The Montreux Declaration

- 27th International Conference of Data Protection and Privacy Commissioners
- 2005-09-14/16 in Montreux, Switzerland
- “The protection of personal data and privacy in a globalised world: a universal right respecting diversities” [ICDPPC 2005]
- 11 principles

11 Principles of the Montreux Declaration

- Lawful and fair data collection and processing,
- Accuracy,
- Purpose-specification and –limitation,
- Proportionality,
- Transparency,
- Individual participation and in particular the guarantee of the right of access of the person concerned,
- Non-discrimination,
- Data security,
- Responsibility,
- Independent supervision and legal sanction,
- Adequate level of protection in case of transborder flows of personal data.

11 Principles of the Montreux Declaration

- Lawful and **fair data collection and processing**,
- Accuracy,
- **Purpose-specification and -limitation,**
- **Proportionality**,
- Transparency,
- **Individual participation and in particular the guarantee of the right of access of the person concerned,**
- Non-discrimination,
- Data security,
- **Responsibility,**
- Independent supervision and legal sanction,
- Adequate level of protection in case of transborder flows of personal data.

mobile business

Data scarcity and Control by the user

- **Data scarcity**
  - Only collect and process data that are needed for the service/process
  - Use/Develop technologies that provide the service using less data.
  - derived from
    - Fair data collection and processing,
    - Purpose-specification and –limitation,
    - Proportionality
- **Control by the User**
  - Let users decide, when and where data are flowing
  - Derived from
    - Individual participation and in particular the guarantee of the right of access of the person concerned
    - Responsibility

Major trends in ICT Applications, Privacy & Security

- ICT gets ever closer to people
  - Provides more and more sensitive services
  - Grows into an extension of the human
  - Collects more and more data
- Businesses/States/Governments try to collect more and more data
  - Personalised and Customized Services
  - Customer profiling
  - Me-too Approach from governments for {anti-terror; law enforcement; security; safety; surveillance}
- Privacy regulation tries to define a space of individual freedom
  - Informational Self-determination
  - Regulation on Data-Flows and Identification
  - Right to secure technology for confidentiality and integrity (German Constitutional Court, 2008-02-27)

mobile business

Agenda

- Privacy in a data intensive Information Society
- Identity Management
- Multilateral Security
- Enhancing Privacy via Intermediary Architectures and Choice
- Learnings for Development, Research, Standardisation
- Conclusions & Outlook

Identity Management (IdM)
2 sides of a medal with enormous economic potential

- **Organisations** aim to sort out
  - User Accounts in different IT systems
  - Authentication
  - Rights management
  - Access control
  -
- **Unified identities** help to
  - ease administration
  - manage customer relations
- **Identity management systems**
  - ease single-sign-on by unify accounts
  - solve the problems of multiple passwords

- **People** live their life
  - in different roles (professional, private, volunteer)
  - using different identities (pseudonyms): email accounts, SIM cards, eBay trade names, chat names, 2ndLife names, …)
- **Differentiated identities** help to
  - protect
    - privacy, especially anonymity
    - personal security/safety
  - enable reputation building at the same time
- **Identity management systems**
  - support users using role based identities
  - help to present the “right” identity in the right context

Identity Management (IdM)
2 sides of a medal with enormous economic potential

- **People** live their life
  - in different roles (professional, private, volunteer)
  - using different identities (pseudonyms): email accounts, SIM cards, eBay trade names, chat names, 2ndLife names, …)
- **Differentiated identities** help to
  - protect
    - privacy, especially anonymity
    - personal security/safety
  - enable reputation building at the same time
- **Identity management systems**
  - support users using role based identities
  - help to present the “right” identity in the right context

- **Organisations** aim to sort out
  - User Accounts in different IT systems
  - Authentication
  - Rights management
  - Access control
  -
- **Unified identities** help to
  - ease administration
  - manage customer relations
- **Identity management systems**
  - ease single-sign-on by unify accounts
  - solve the problems of multiple passwords

Digital (mobile) Identities

- A concept that **links** a „token“ from the *digital/syntactical world* to an object in the *real/semantical world* **(idem identity)**

Authentication

Authentication

- Accompanied by a set of **properties** and attributes **(ipse identity)**

Interests

Position

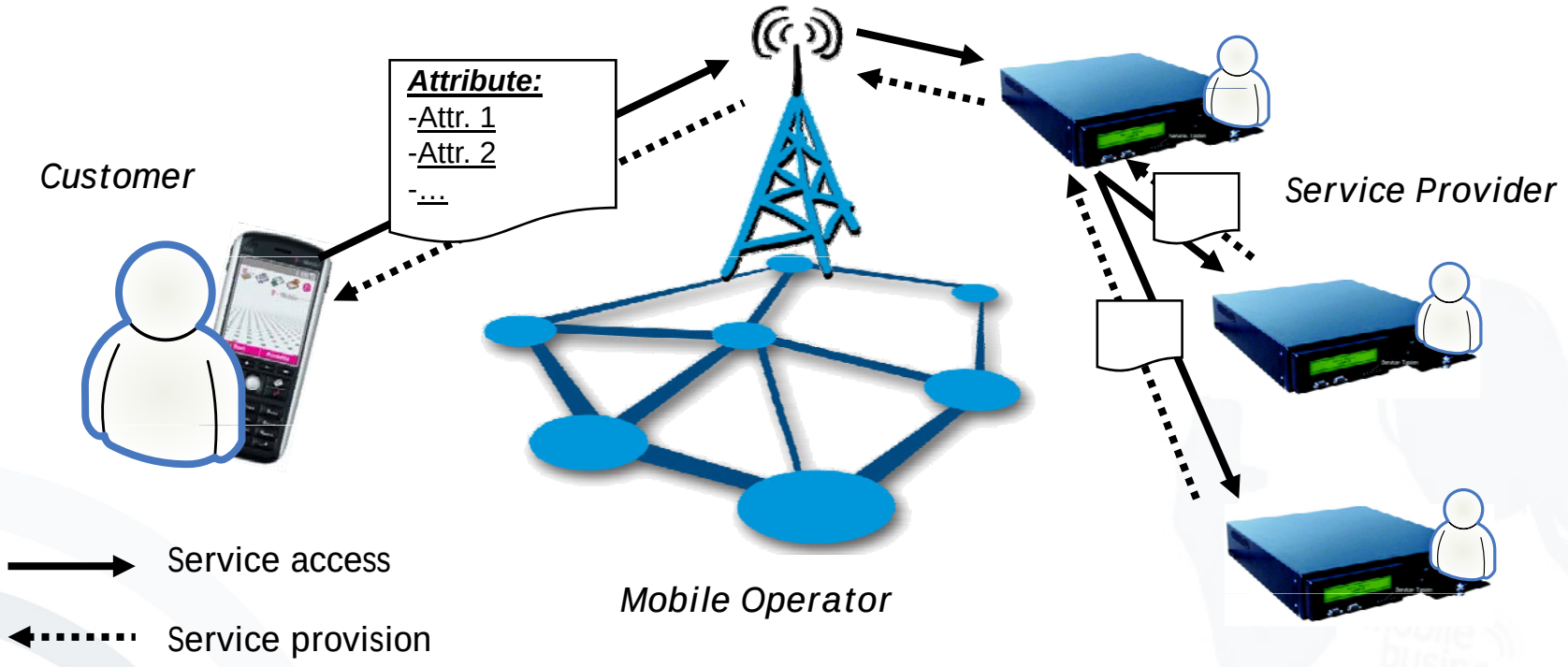
Age

Income

Many players aim for identities, e.g. Google

- Offers search combined with advertisements (Google Search)
- Offers location based advertising (Google Earth, Google Maps)
- Issues email accounts (Gmail)
- Generalises accounts (Google Accounts)
- Offers a Portal Hosting Service (YouTube)
- Develops a mobile operating system (Android)
- Implements communication infrastructures (WLAN in Mountain View and San Francisco)
- Implements Payment System (Google Checkout)
- Builds up Community Services (jaiku)
- ...

User controlled transfer of Attributes



Identity Management via Application Creep

- Perhaps the only way for an identity management infrastructure to become successful:
  - Creep in via an application
  - Creep to further applications
- ➢ Nice from an informatics point of view: "General informatics tools and principles get reused."
- ➢ Problematic from a privacy point of view
- ➢ A challenge for IT Security

mobile business

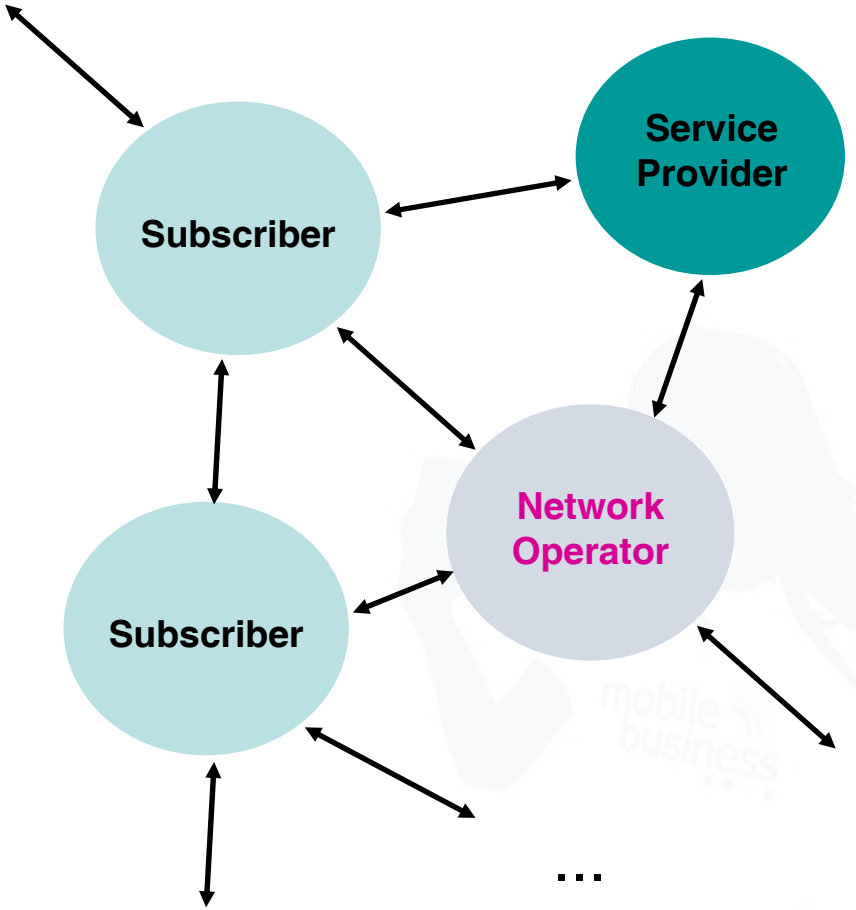
Agenda

- Privacy in a data intensive Information Society
- Identity Management
- Multilateral Security
- Enhancing Privacy via Intermediary Architectures and Choice
- Learnings for Development, Research, Standardisation
- Conclusions & Outlook

Security for whom?

- Technology?
  - Devices
  - Infrastructures
- Processes?
  - Transactions
  - Payment
- People?
  - Citizens
  - Employees
  - Customers
  - “Security is becoming a people problem.” [Roger Needham, 2001]

Different parties with different interests in communication networks



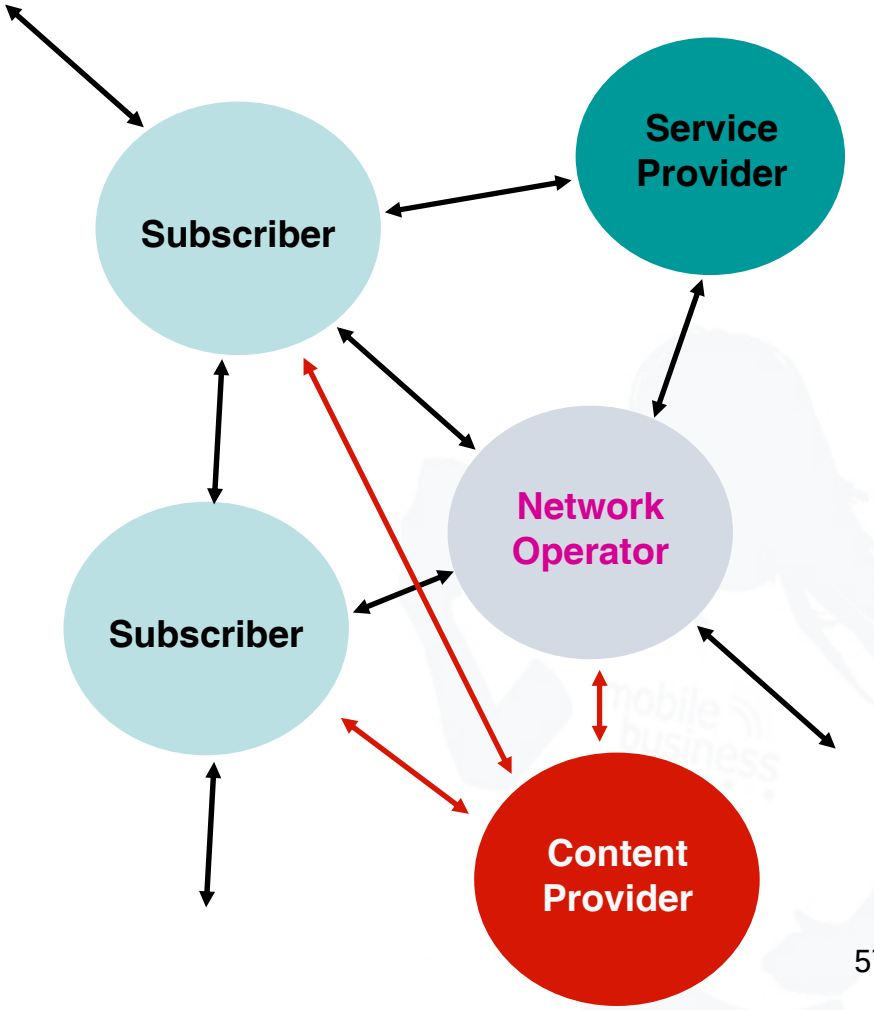
Other examples

- Customers/ Merchants
- Communication partners
- Citizens/ Administration

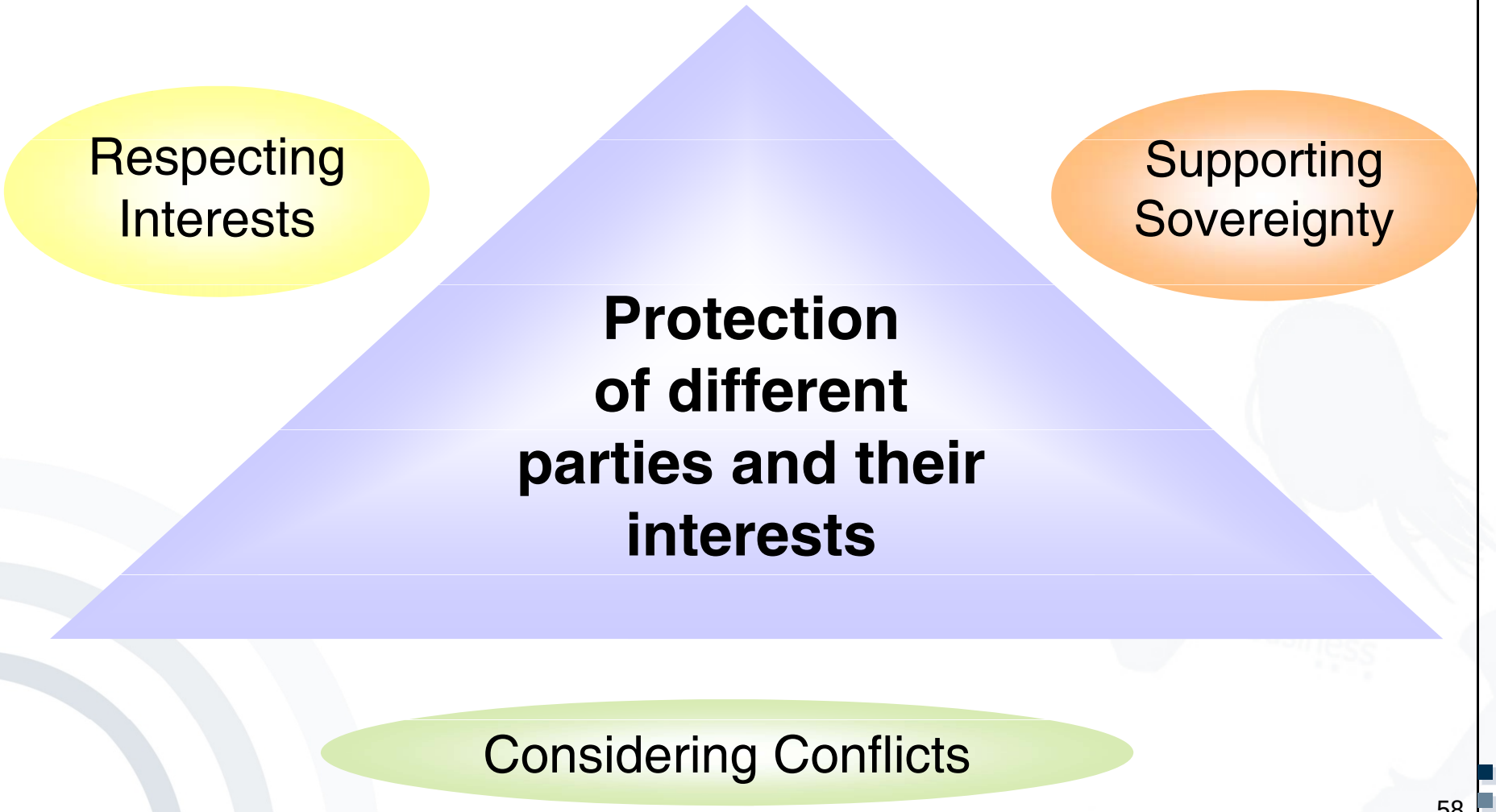
… in E/M-commerce

… in a world of consortia

- more partners
- more complex relations



Multilateral Security



mobile business

Multilateral Security considers conflicts

Respecting Interests

- Parties can define their own **interests**.
- Conflicts can be **recognised** and **negotiated**.
- Negotiated **results** can be reliably **enforced**.

Supporting Sovereignty

- Requiring each party to **only minimally trust** in the honesty of **others**
- Requiring **only minimal or no trust in technology** of others

Protection of **different parties** and their **interests**

mobile business

Agenda

- Privacy in a data intensive Information Society
- Identity Management
- Multilateral Security
- Enhancing Privacy via Intermediary Architectures and Choice
- Learnings for Development, Research, Standardisation
- Conclusions & Outlook

PRIME LBS Application Prototype

- **Enhance privacy for typical LBS**
  - **Pharmacy search (“pull”)**
  - **Pollen warning (“push”)**
- **Address wide user range by making only few requirements on the existing infrastructure**
  - **Version 1 simple WAP mobile phone**
  - **Version 2 Java phone**
- **Considering B2B scenarios in the value chain**

The issues in a bit more detail

- Location-based services are a promising business
  - Market penetration of GPS phones still limited
  - Mobile operator may step in based on Cell ID information

- Several challenges
  - Privacy problems
  - Regulation, e.g. of the handling of personal information (and mobile services in general)
  - Business constraints
    - Easy integration into existing infrastructure
    - Applicability to a wide range of business models
    - Adaptability for different market structures

Research Objectives

- **Investigate Requirements of Stakeholders in LBS Scenario**
  - **From economic, legal and individual/organizational perspectives**
- **Design a Middleware Architecture and Prototype Implementation**
  - **Architecture derived from requirements**
  - **Two implementation iterations, spanning mobile phone generations (WAP, J2ME)**
- **Analyse and Evaluate Implementation**
  - **Project-Internal Evaluation**
  - **Experiences and observations from implementation and deployment**

Research Approach, Methodology

- **Case Study**
  - **Identifies LBS as a scenario where PETs can be beneficial for all involved parties**
  - **Prototype design, implementation, deployment and development of commercial version covered**

- **Design Science**
  - **Based on requirements and founded on theory**
  - **Architecture and several implementation generations**
  - **Several evaluation angles**

LBS
Involved Parties

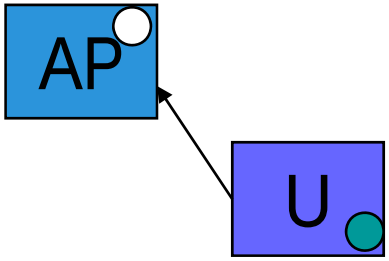
AP Location-Based Service Application Provider, a special type of value adding service provider in mobile networks

U User, usually a person, but could also be a business entity, or even a vehicle or container

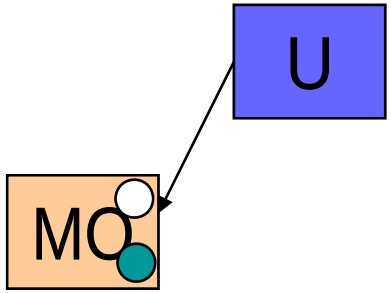
LI Location Intermediary, a Party with the business of mediating between LBS provider and operators; it can also perform privacy functionality.

MO Operator of a mobile network, that uses its infrastructure to localize users.

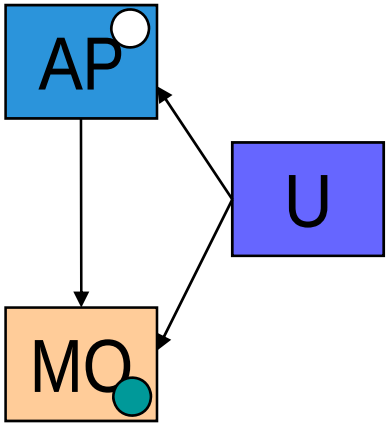
LBS Background Information
Four Different Business Models



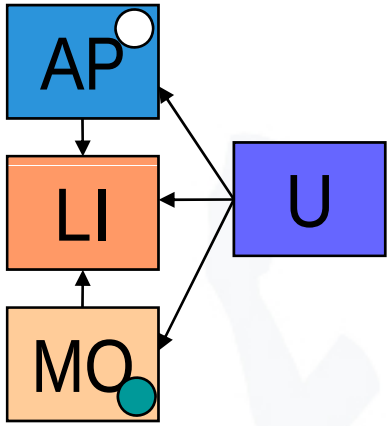
1. Direct localization scenario



2. Operator-portal scenario



3. Application provider scenario



4. Intermediary scenario

○ Service

● Location Source

mobile business

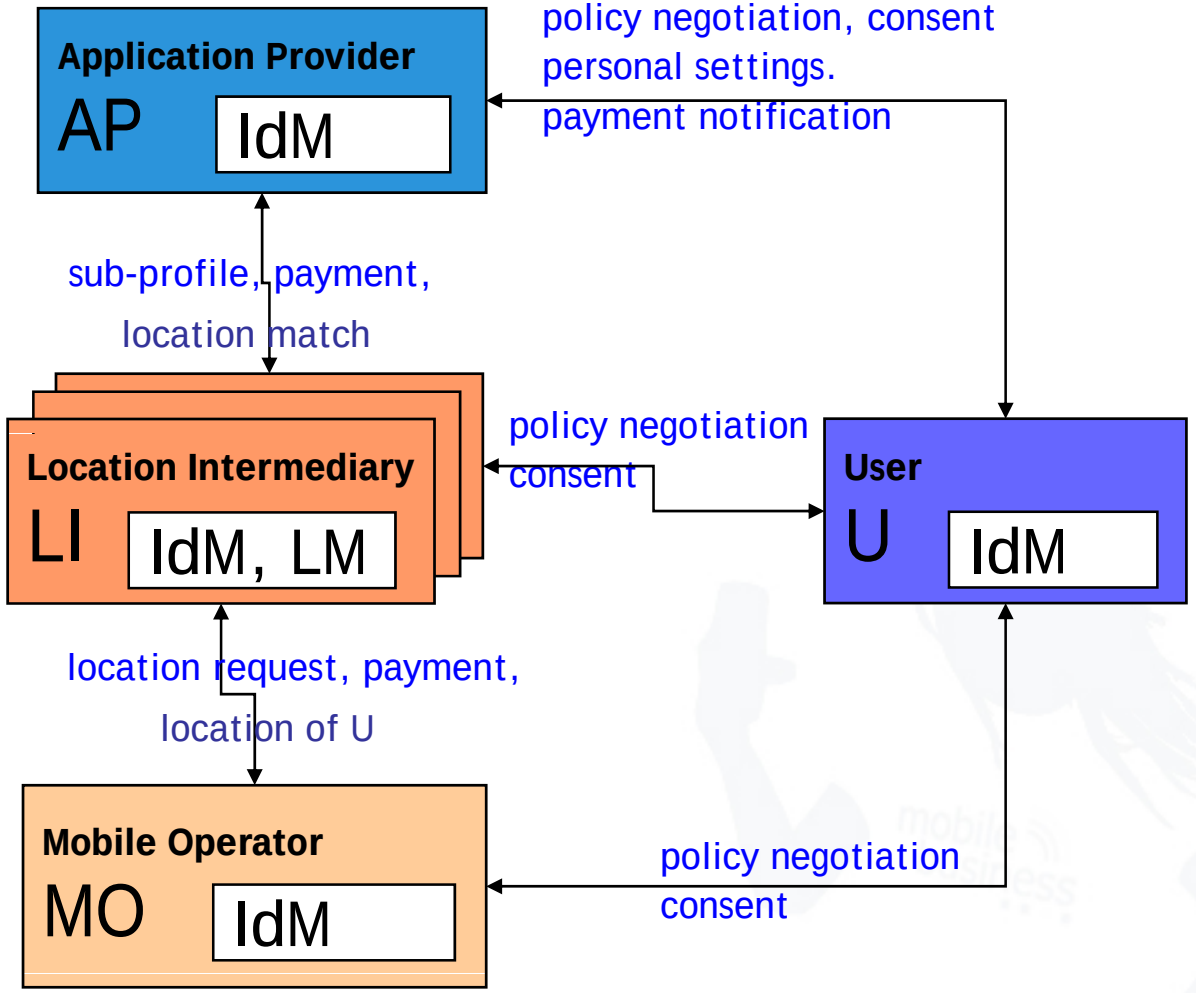
LBS Architecture including an Intermediary

- An architecture for providing LBS consists of a location source (LS) that is queried for user U's location, a server LBS_S operated by the application provider (AP) that provides the LBS application, and of client LBS_C owned by a user known as U.
- We extended this basic setting with two new application independent components.
  - The first one is an identity management component (IdM) providing users with unlinkable pseudonyms for different business parties.
  - The second component is the location matcher (LM). Its purpose is the secure implementation of push services. IdM and LM are used by the location intermediary (LI) to mediate between AP's localization requests and LS at mobile operator MO. The user is known under distinct pseudonyms to MO and AP. Communicating through LI with IdM and LM, neither MO nor AP can link the user's pseudonyms.

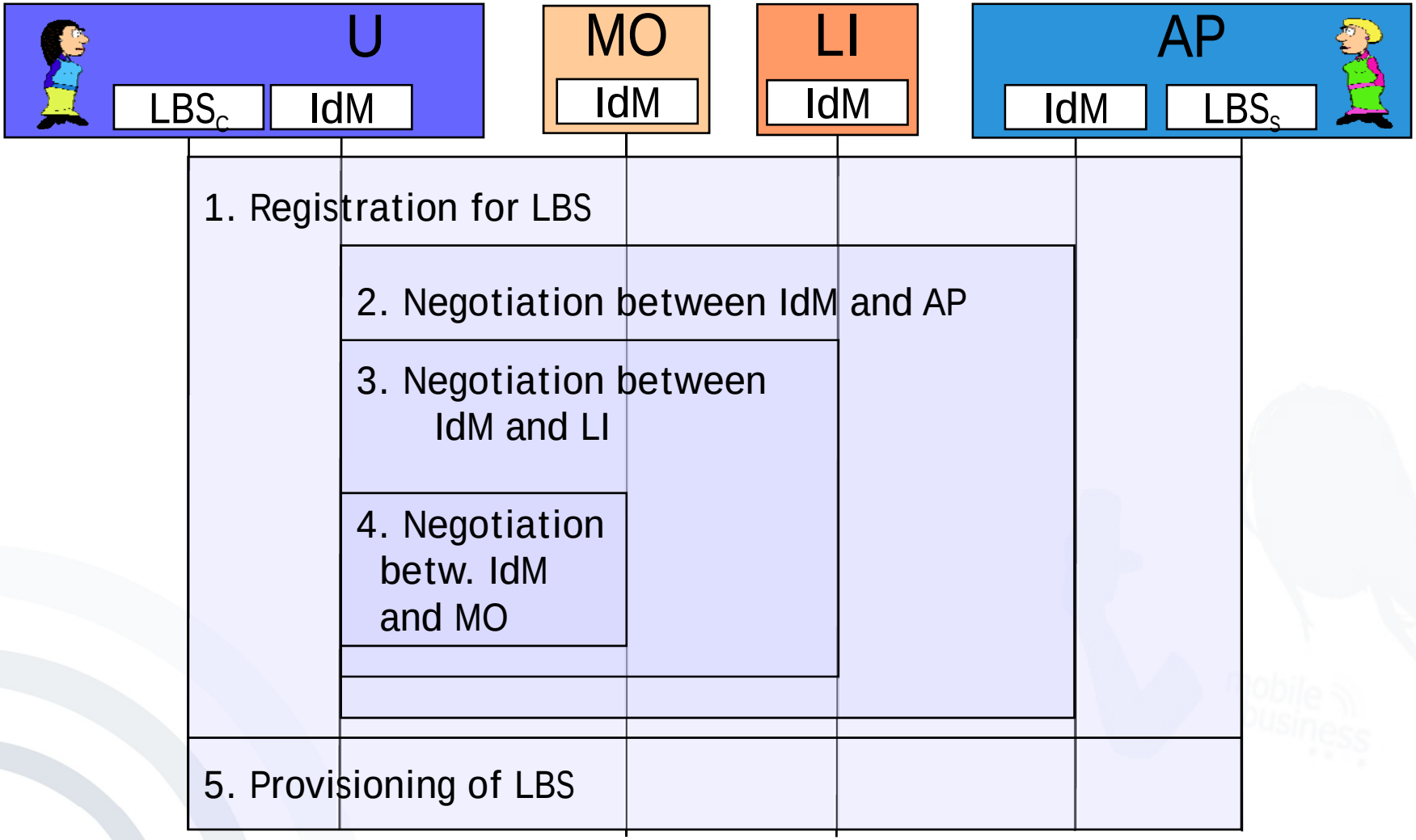
Location & Identity Management by Intermediaries

Intermediary Functions

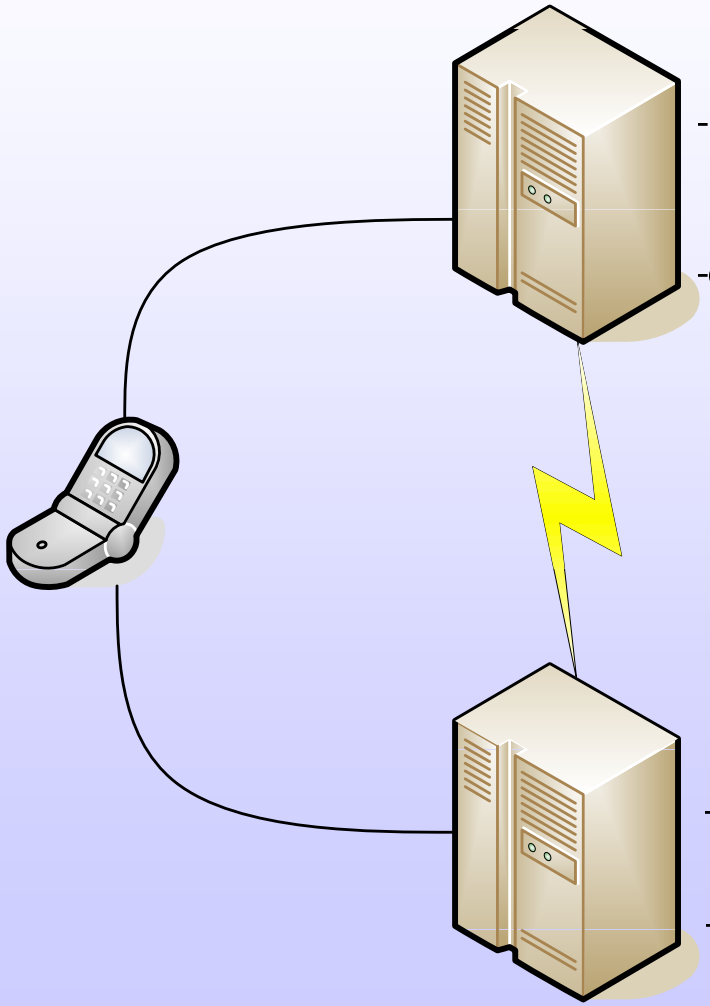
- Identity management (IdM)
  - Providing users with unlinkable pseudonyms for different business partners
- Location matching (LM)
  - Providing AP with location info only when needed, e.g. for a push services



LBS architecture including an Intermediary



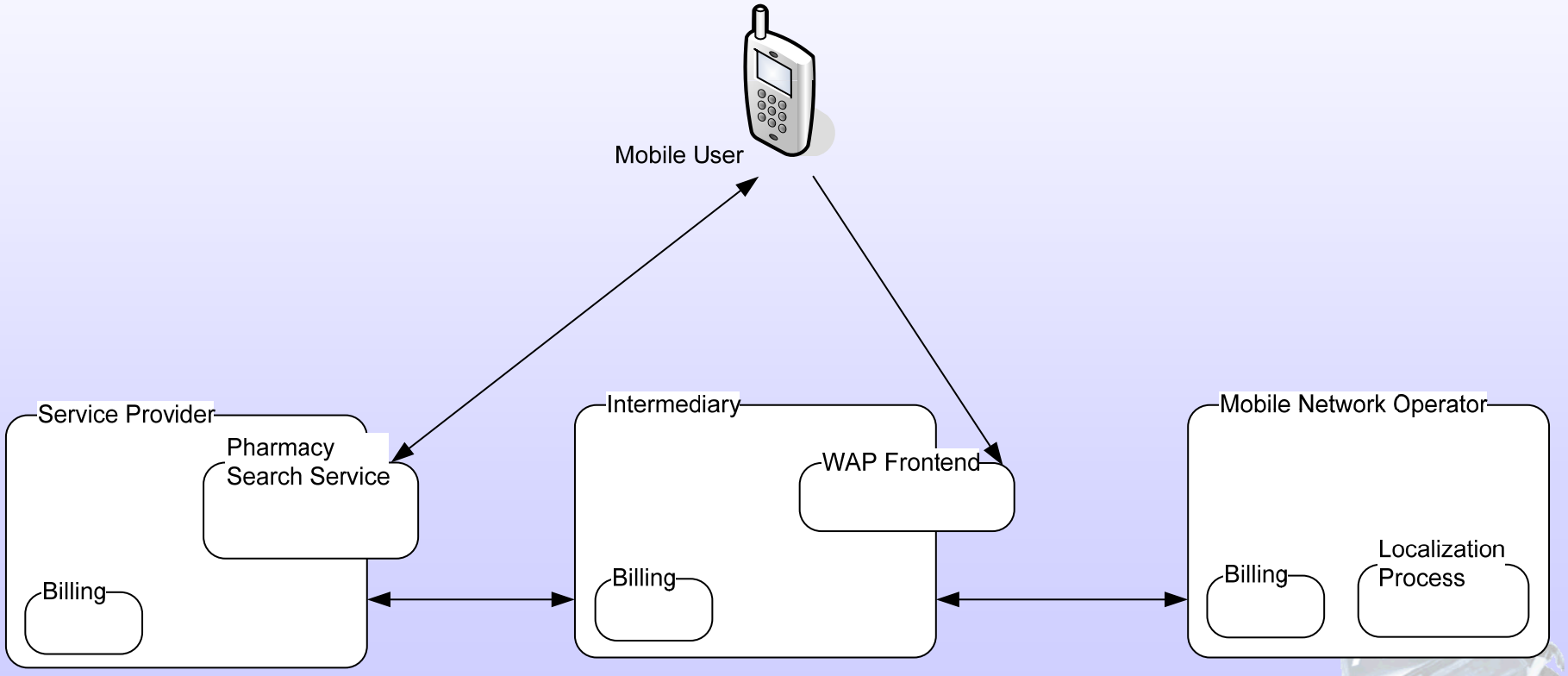
Conventional LBS Deployment



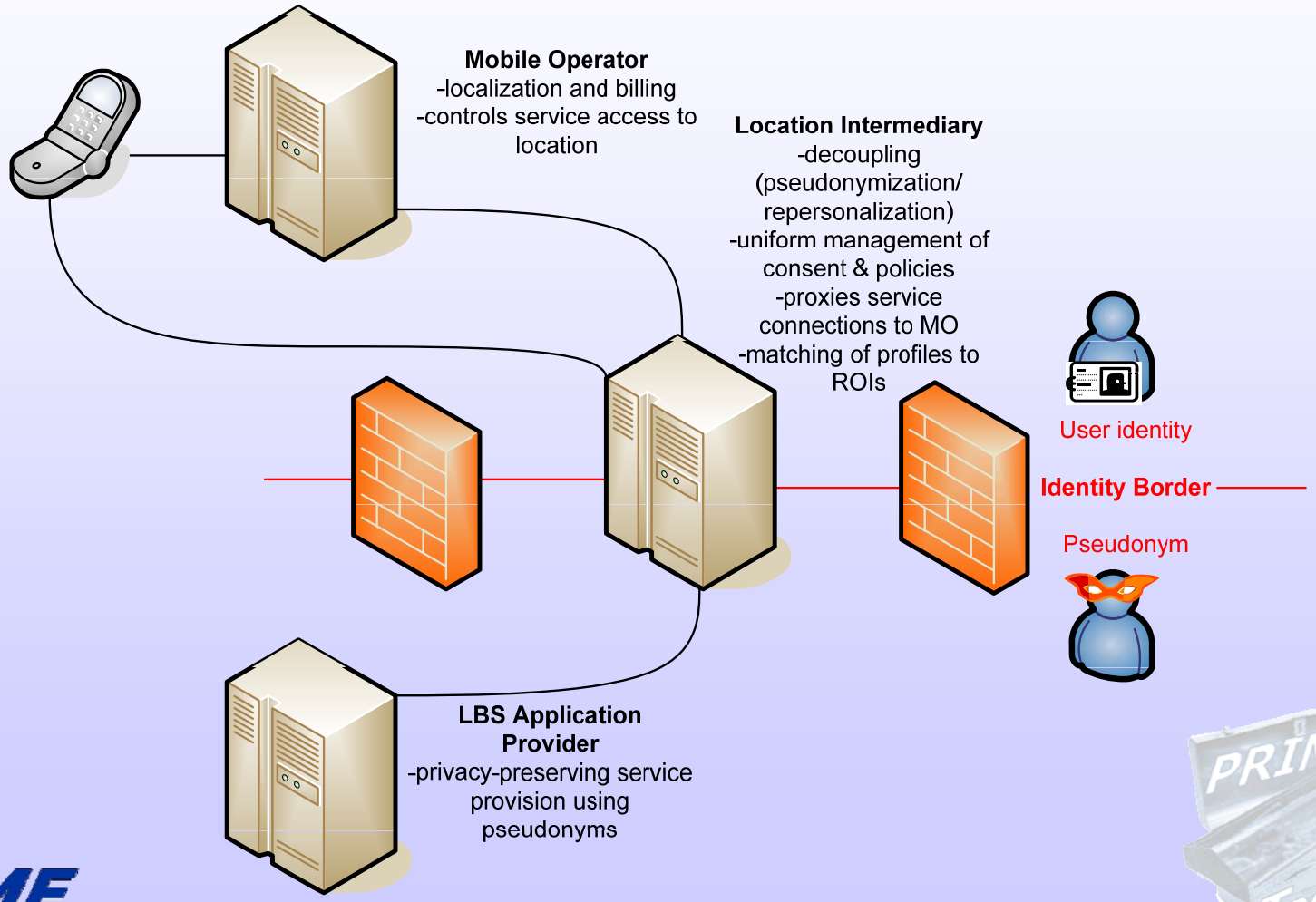
Mobile Operator
-learns user's services & all usage patterns
-can monitor sent notifications
-can derive e.g. allergies

LBS Application Provider
-usage patterns
-needs to identify user for billing
-movement profiles
-per service configuration of policies and consent

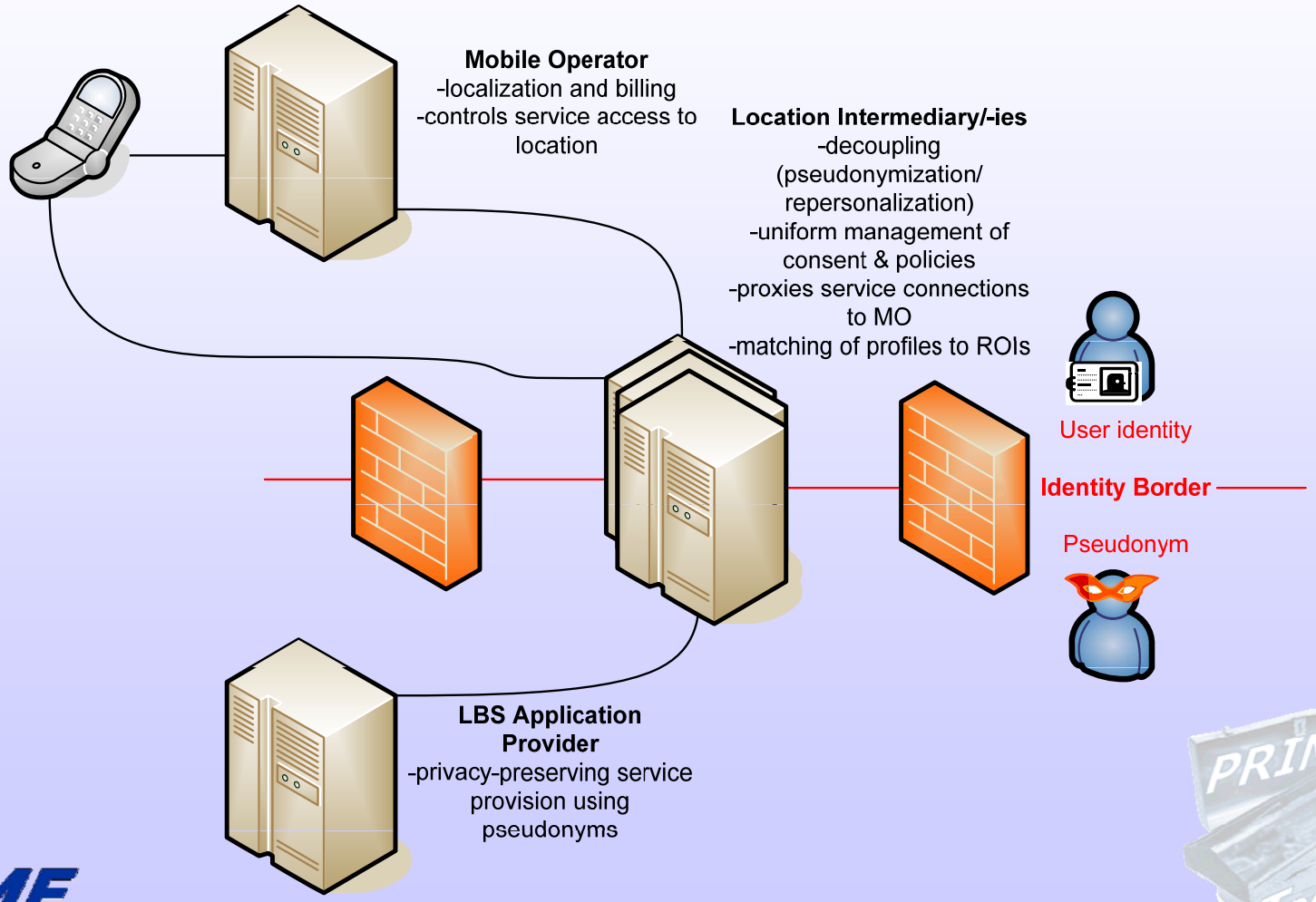
Solution Approach
Intermediary



Intermediary Approach
Architecture Overview



Intermediary Approach
Architecture Overview

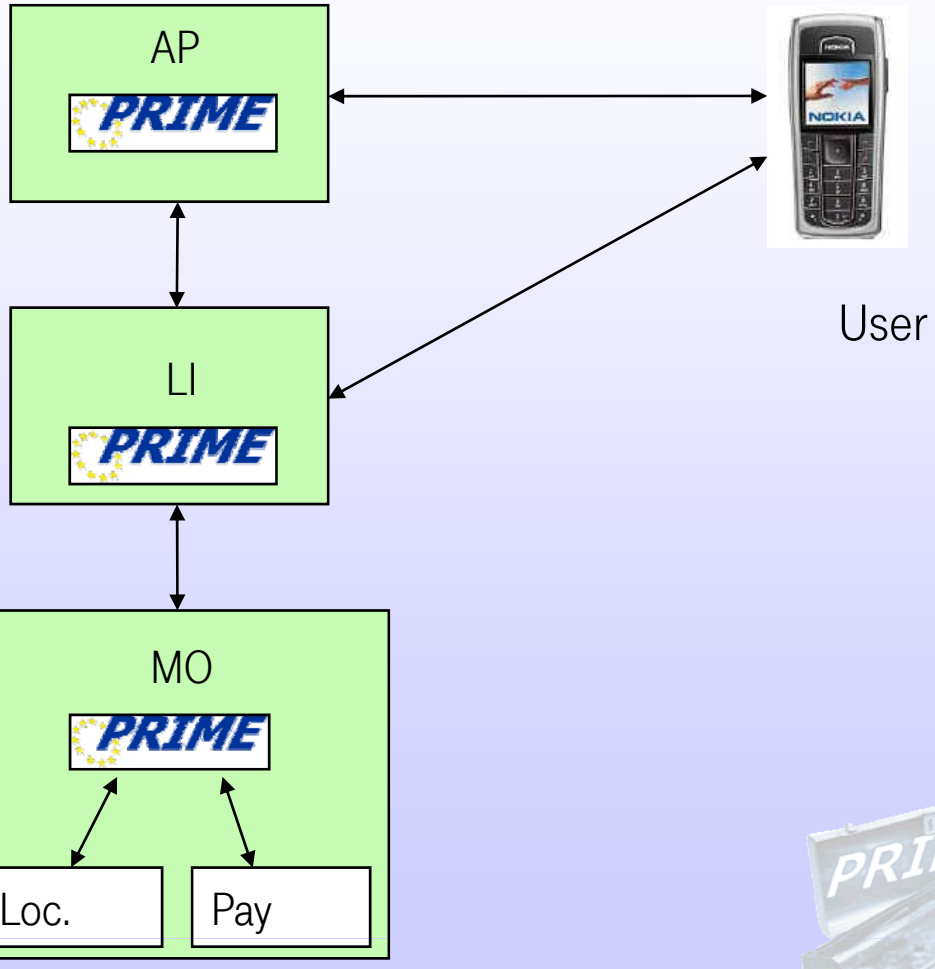


Pharmacy Search

LBS Application Provider
- Pharmacy Search -

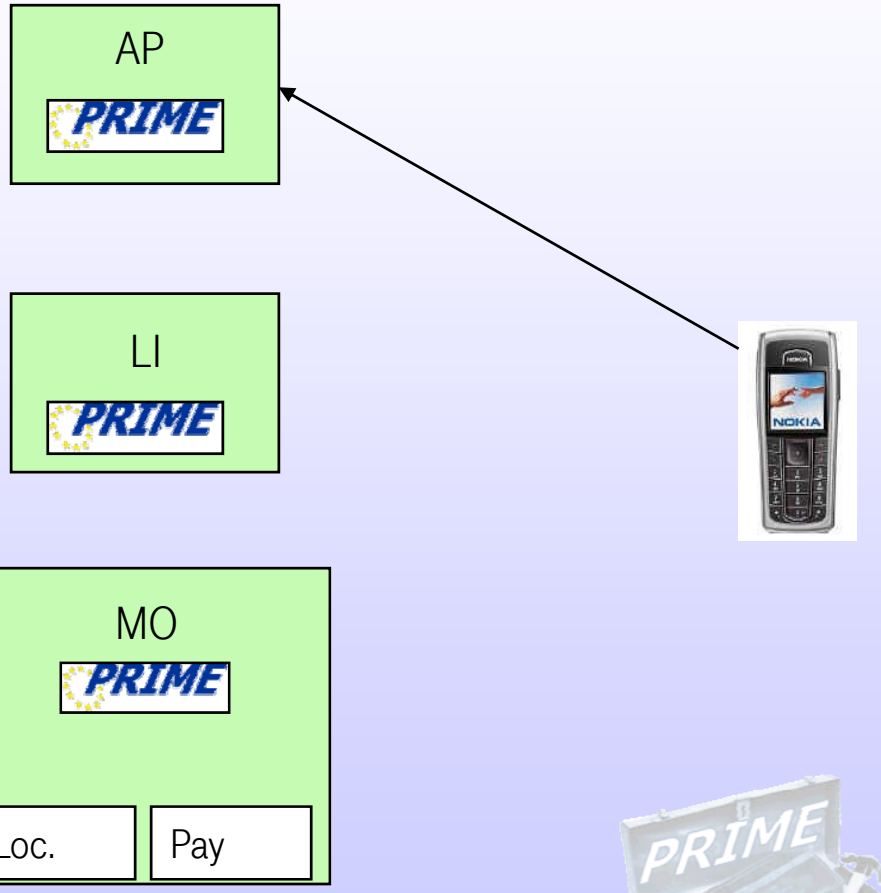
Location Intermediary

Mobile Operator



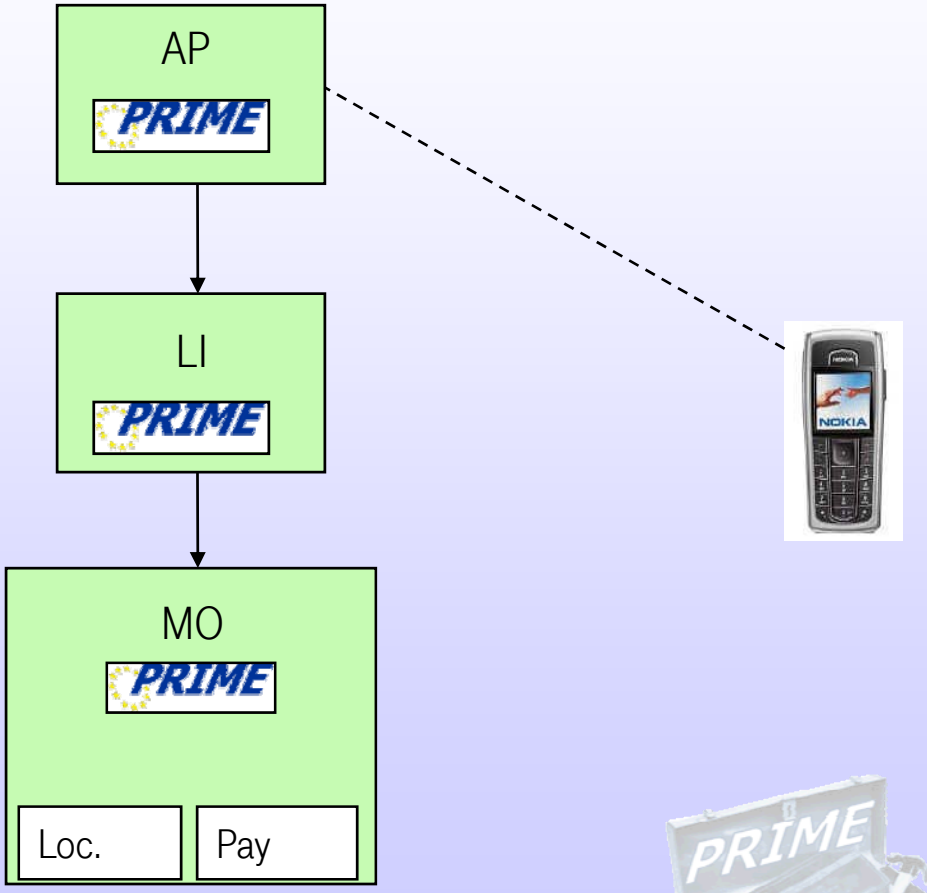
Use Case (Step 1)

- User starts service



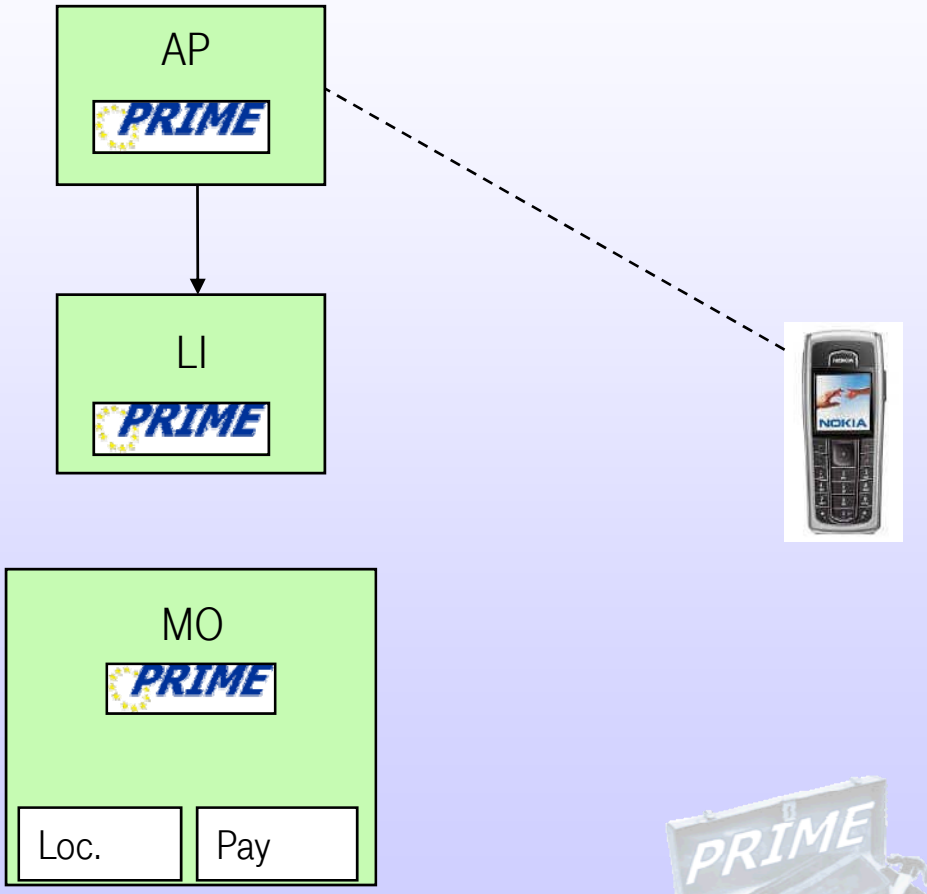
Use Case (Step 2)

- User starts service
- AP requests access handle with user IP
  - LI requests person pseudonym
  - MO resolves user ID
  - LI returns access handle



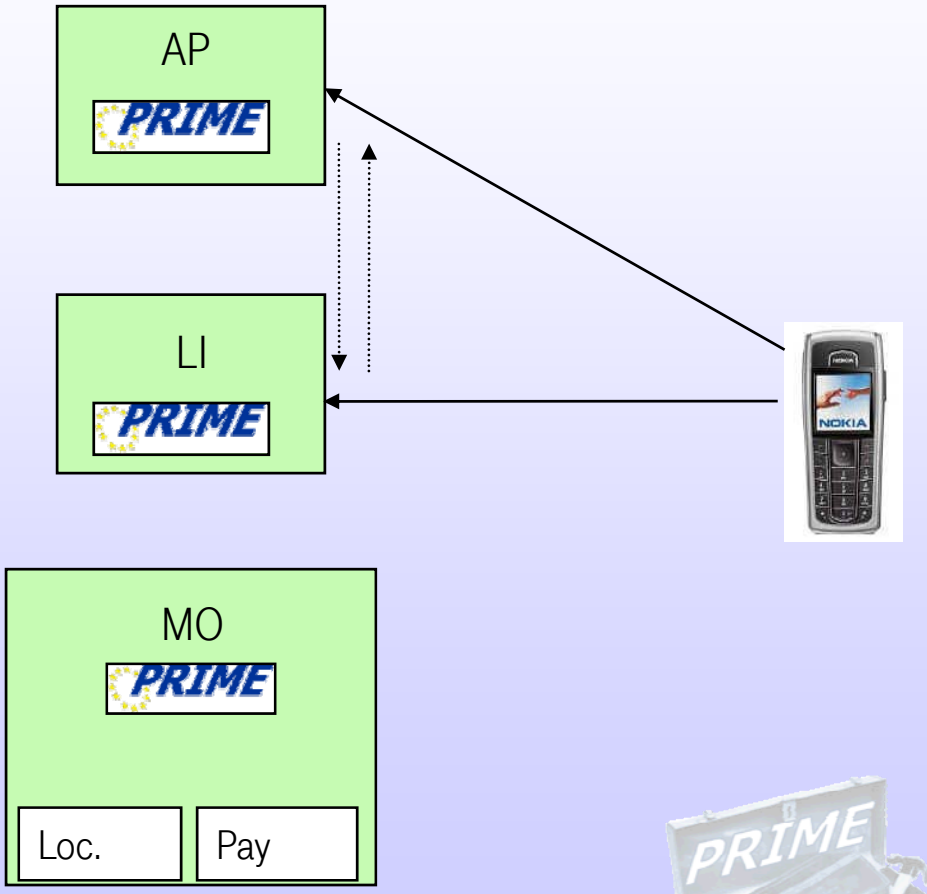
Use Case (Step 3)

- User starts service
- AP requests access handle with user IP
- AP requests location & payment
  - LI's PRIME instance checks policies



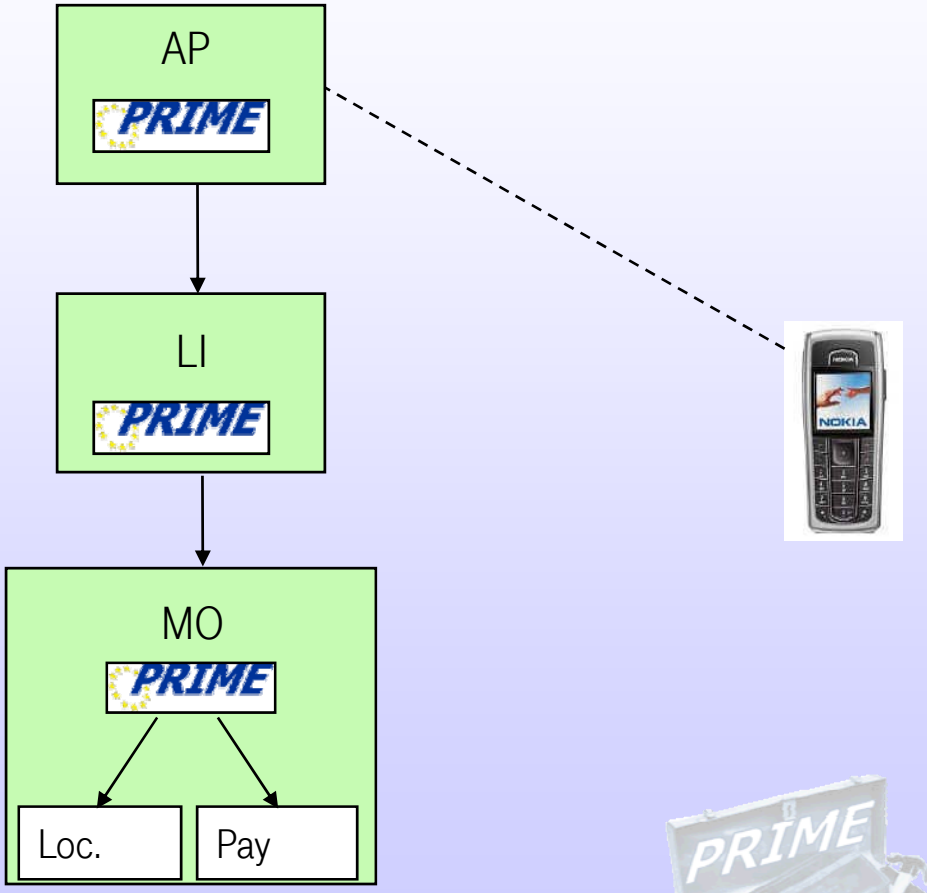
Use Case (Step 4)

- User starts service
- AP requests access handle with user IP
- AP requests location & payment
  - LI's PRIME instance checks policies
  - In case no policy fits:
  - AP sends valid policy proposal to use the service to LI
  - AP then redirects user session to LI
  - User can commit to policy or change policies using WAP browser
  - Session is directed back to AP



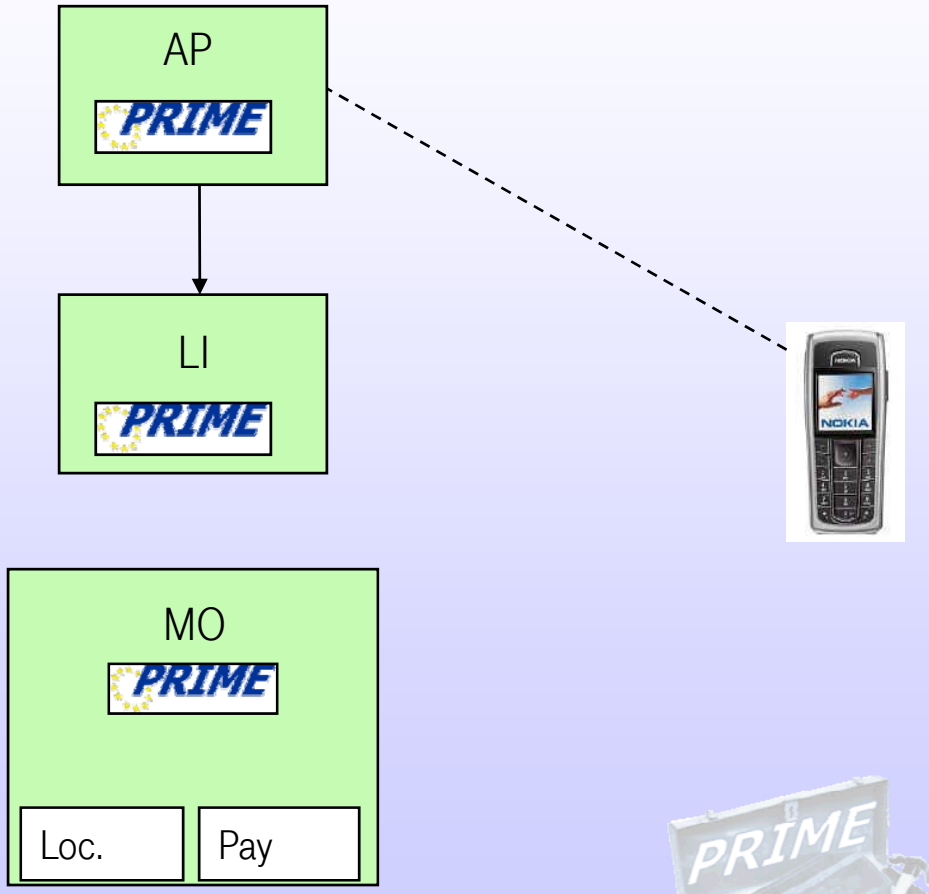
Use Case (Step 5)

- User starts service
- AP requests access handle with user IP
- AP requests location & payment
  - LI's PRIME instance checks policies
  - LI reserves payment and retrieves user position from MO



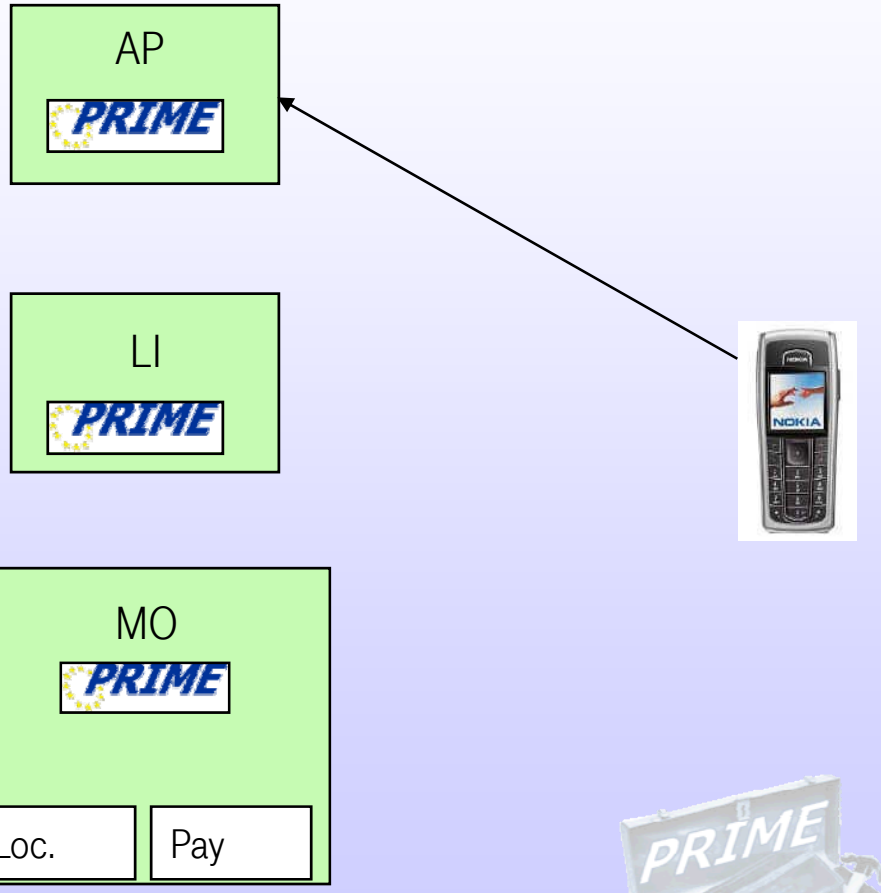
Use Case (Step 6)

- User starts service
- AP requests access handle with user IP
- AP requests location & payment
  - LI's PRIME instance checks policies
  - LI reserves payment and retrieves user position from MO
  - LI provides position & payment handle to AP



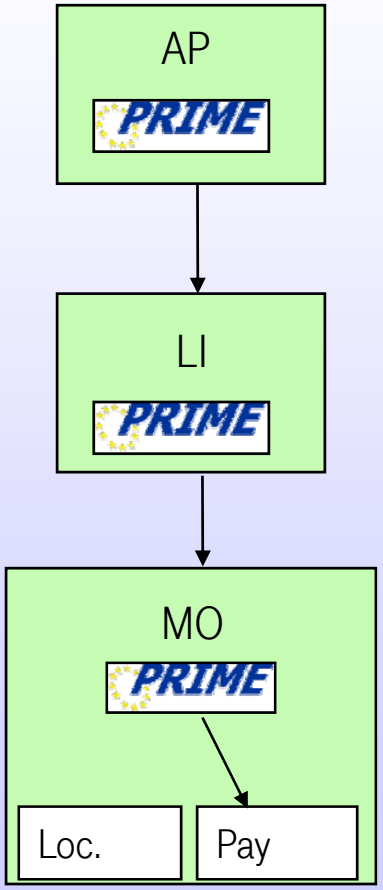
Use Case (Step 7)

- User starts service
- AP requests access handle with user IP
- AP requests location & payment
- AP queries own database and provides result

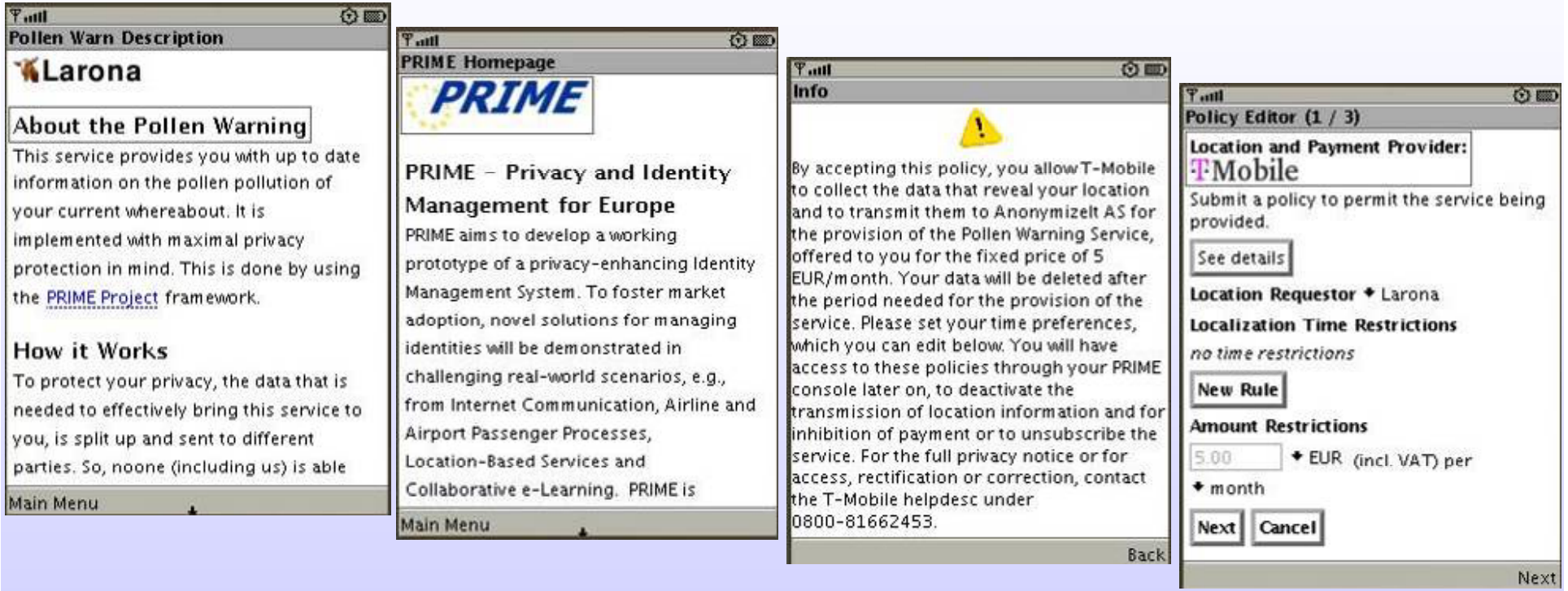


Use Case (Step 8)

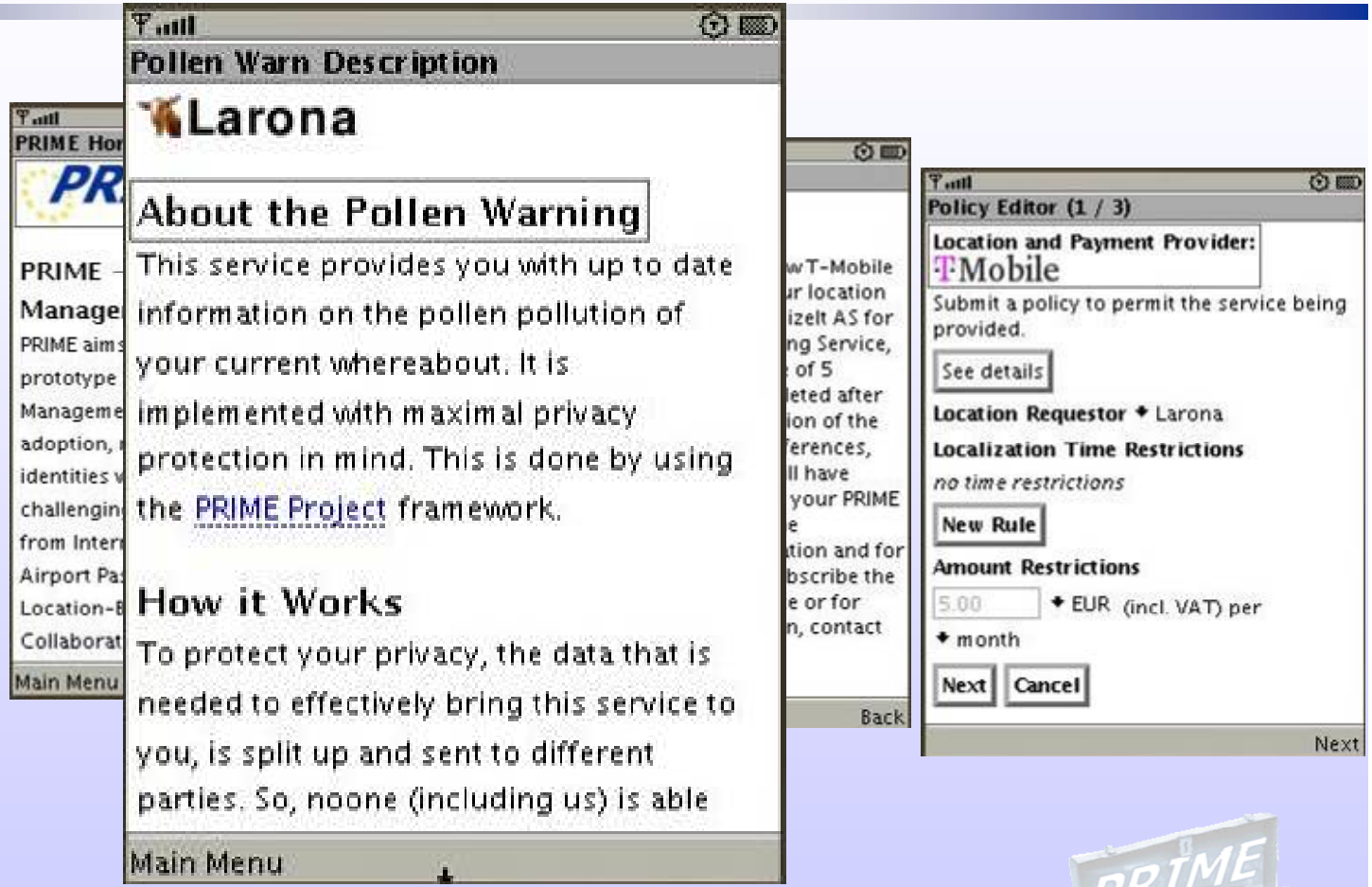
- User starts service
- AP requests access handle with user IP
- AP requests location & payment
- AP queries own database and provides result
- AP commits payment
  - LI forwards request to MO
  - MO performs commit and confirms
  - LI charges AP for localization and transmits debenture to AP



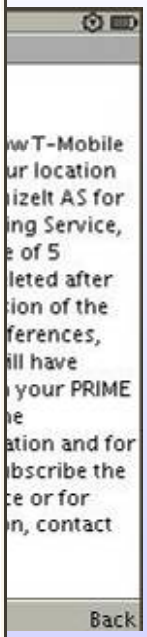
Prototype Screens “Pollen Warning” Overview



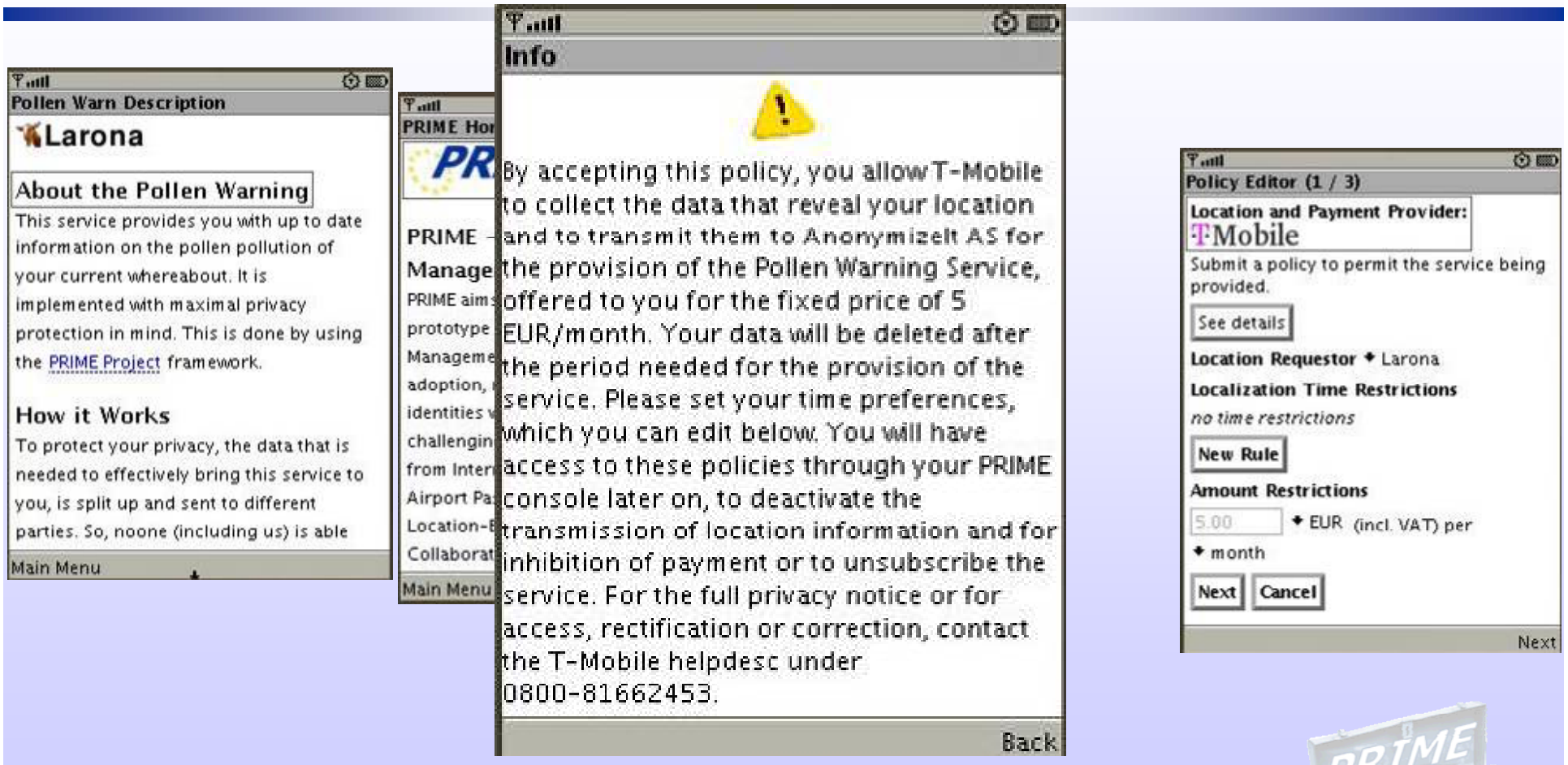
Prototype Screens “Pollen Warning” Information on the Service



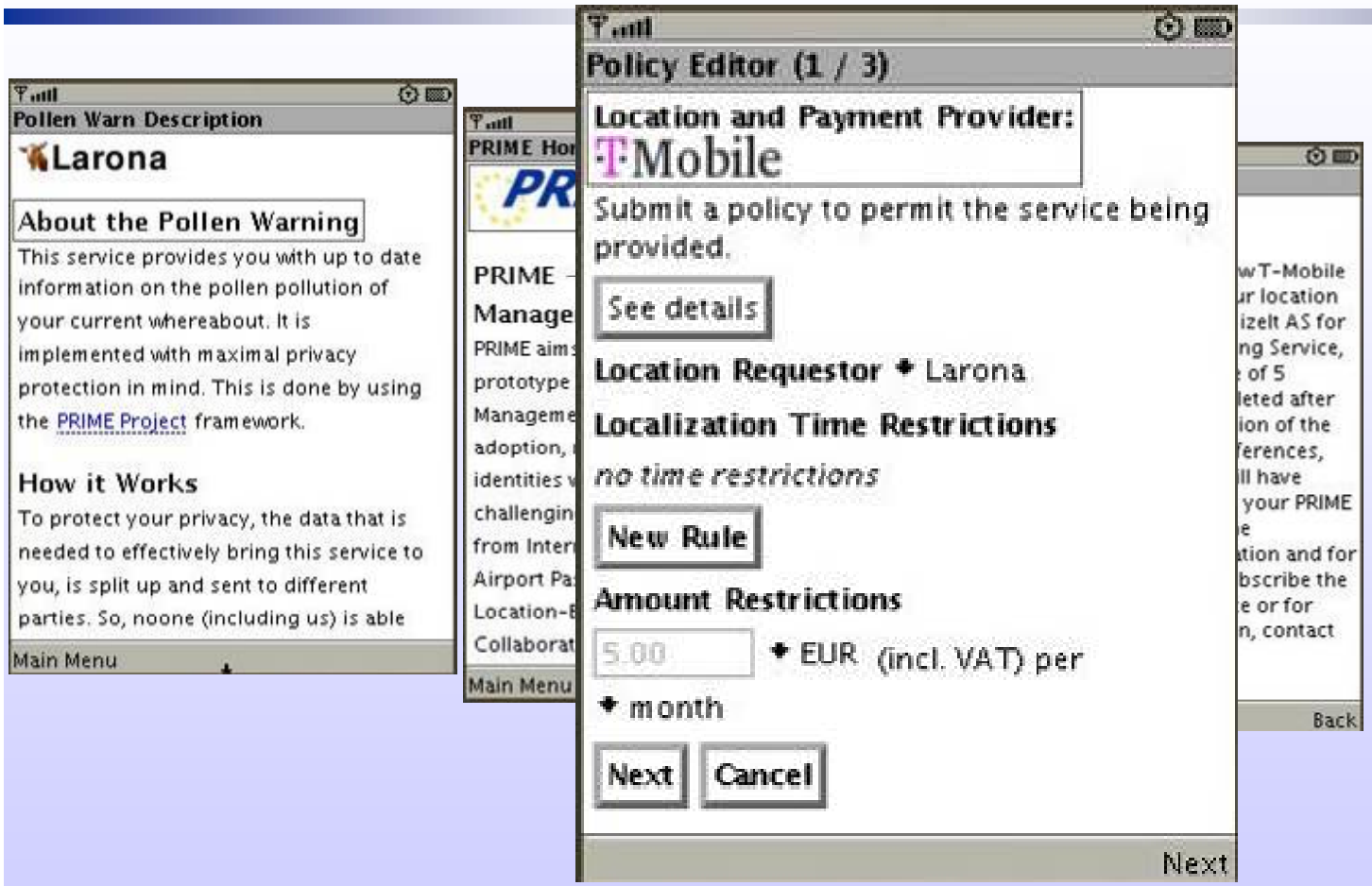
Prototype Screens “Pollen Warning”
A bit of PRIME Advertisement ☺



Prototype Screens “Pollen Warning” Policy Information on data transfer



Prototype Screens “Pollen Warning” Setting your Policy



Suggestions for LBS IdM

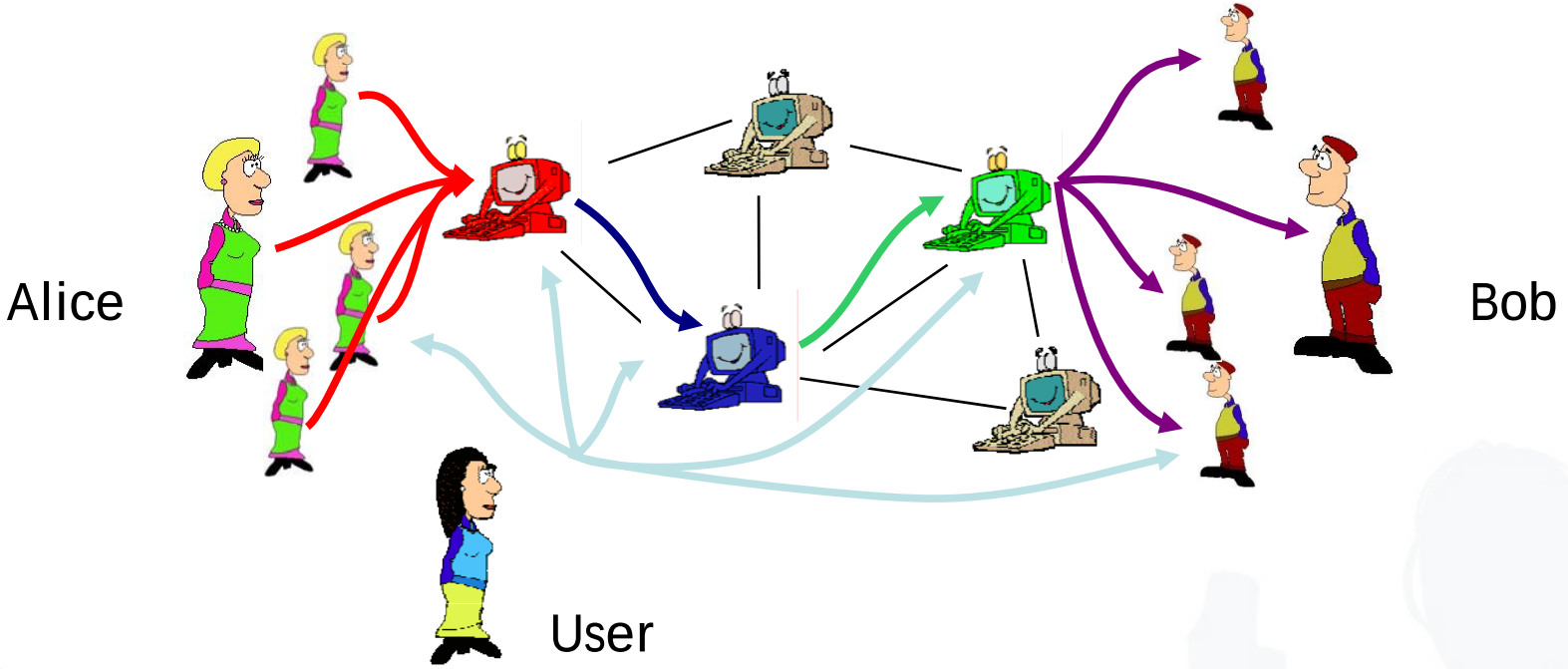
LBS with IdM will need mechanisms to:

1. Conceal attributes not needed
2. Provide location and a few attributes
3. Create reachability with anonymity

Solutions:

1. Should be done with good pseudonymity
2. Can be done with selective IdM
3. Should be done with anonymous channels used for communications

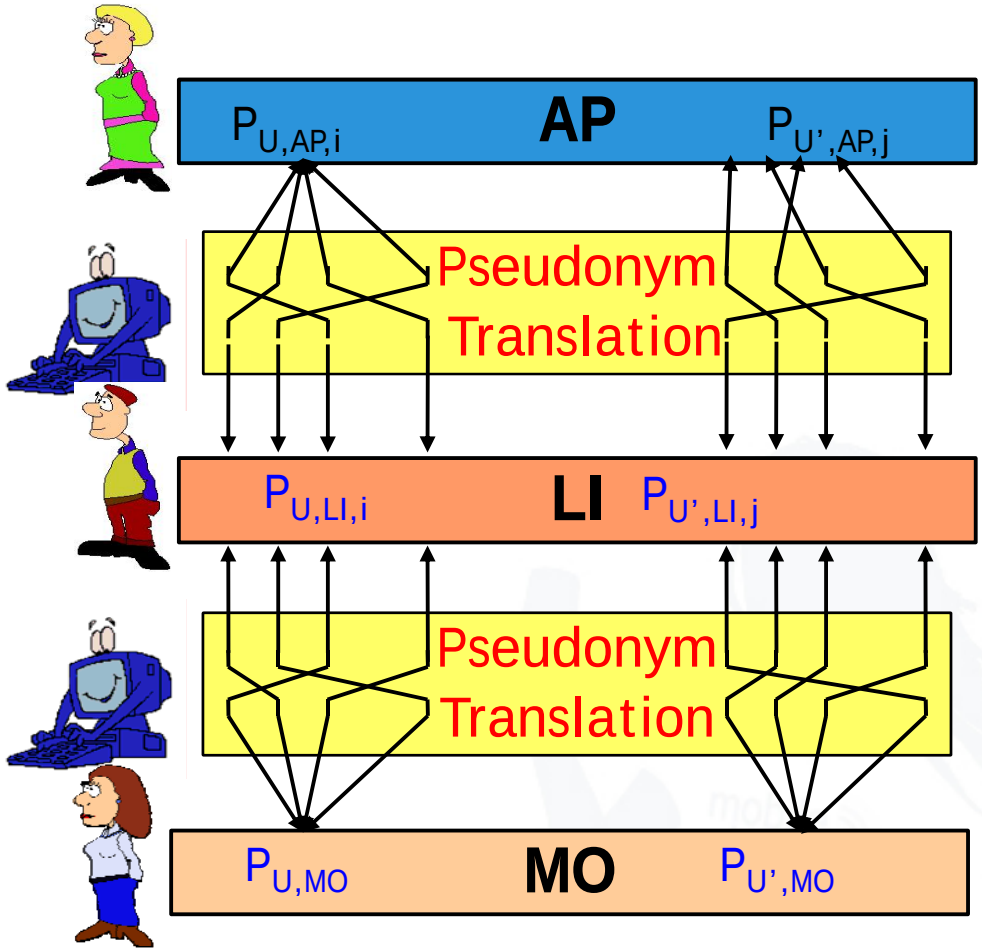
Pseudonym-translating Channels



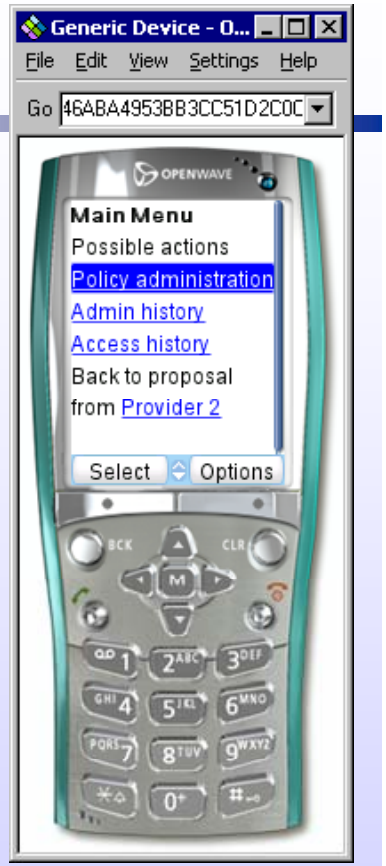
- Conventional anonymous channels (Mixnets & Onion Routing)
  - Alice sets up channel and thus knows Bob.
- Pseudonym-translating Channels (new PRIME concept)
  - User connects one of her pseudonyms with Alice to one of her pseudonyms with Bob.

Pseudonym-translating Channels
Channel switching

- New channels are established
  - in regular time-intervals
  - triggered by MO or U
- No profile re-registration
  - Reduces information known to LI
- With profile re-registration
  - Reduces information known to AP and LI



Case Study Summary

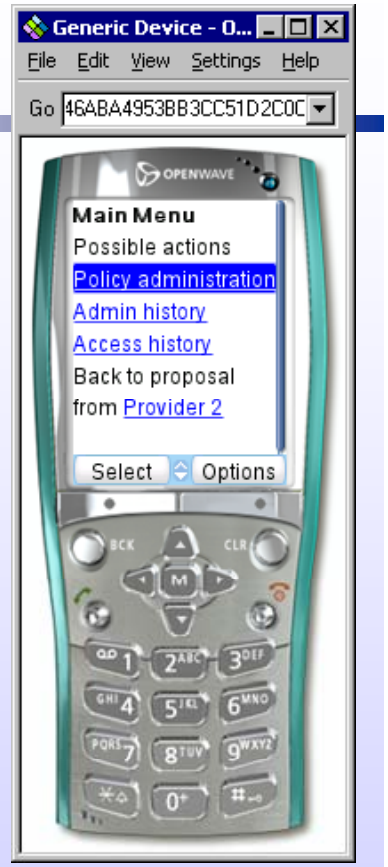


- **Evaluation of prototype assures**
  - **Legal compliance**
  - **Economic benefits**
  - **Technical feasibility**

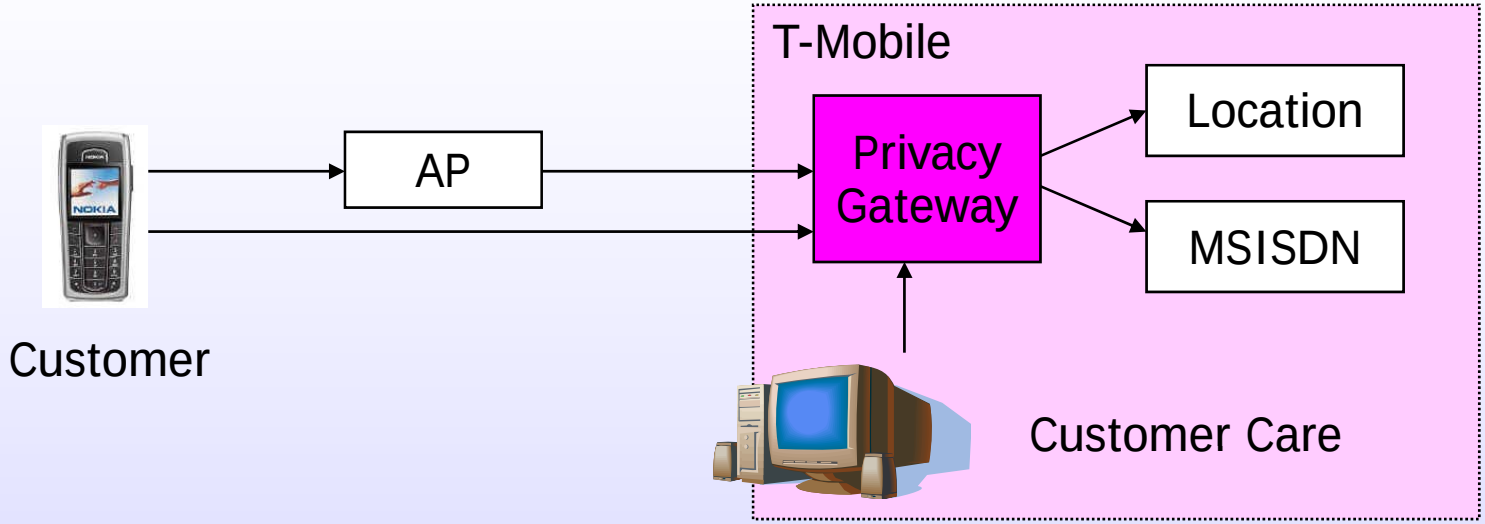
- **First transfers into the real world**
  - **„Privacy Gateway“ infrastructure component deployed at T-Mobile Germany**
  - **Allows subscribers to set**
    - **Which application provider gets data?**
    - **On which days and times?**

Exploitation & Outlook

- First transfers into the real world
  - „Privacy Gateway“ infrastructure component deployed at T-Mobile Germany
  - Allows subscribers to set
    - Which application provider gets data?
    - On which days and times?
- Request for more power on the device for e.g. maintaining one’s own policies
- Computers reflect even closer one’s mind, e.g. one’s trust relations.

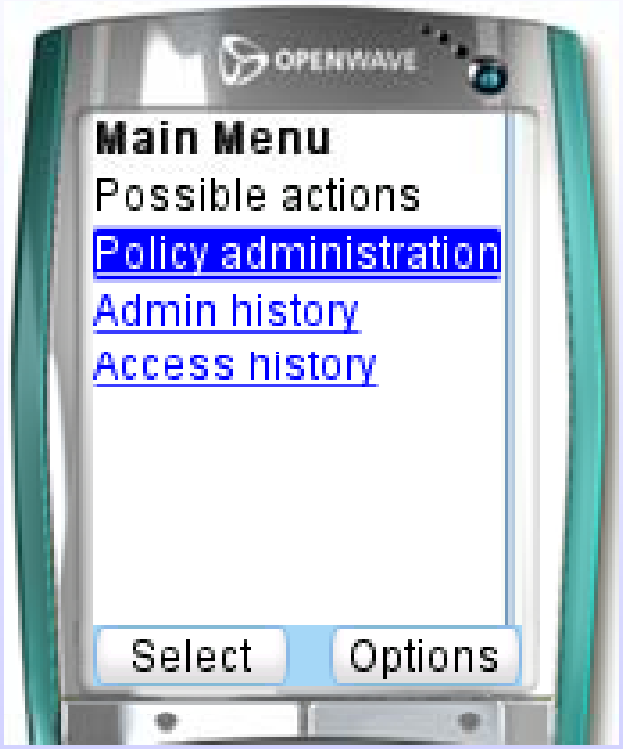


Product Transfer Overview



- WAP configuration
- Customer care web configuration
- SMS configuration:
  - Status: “?” ► 27637
  - Allow: “+provider1” 27637
  - Deny: “-provider1” 27637

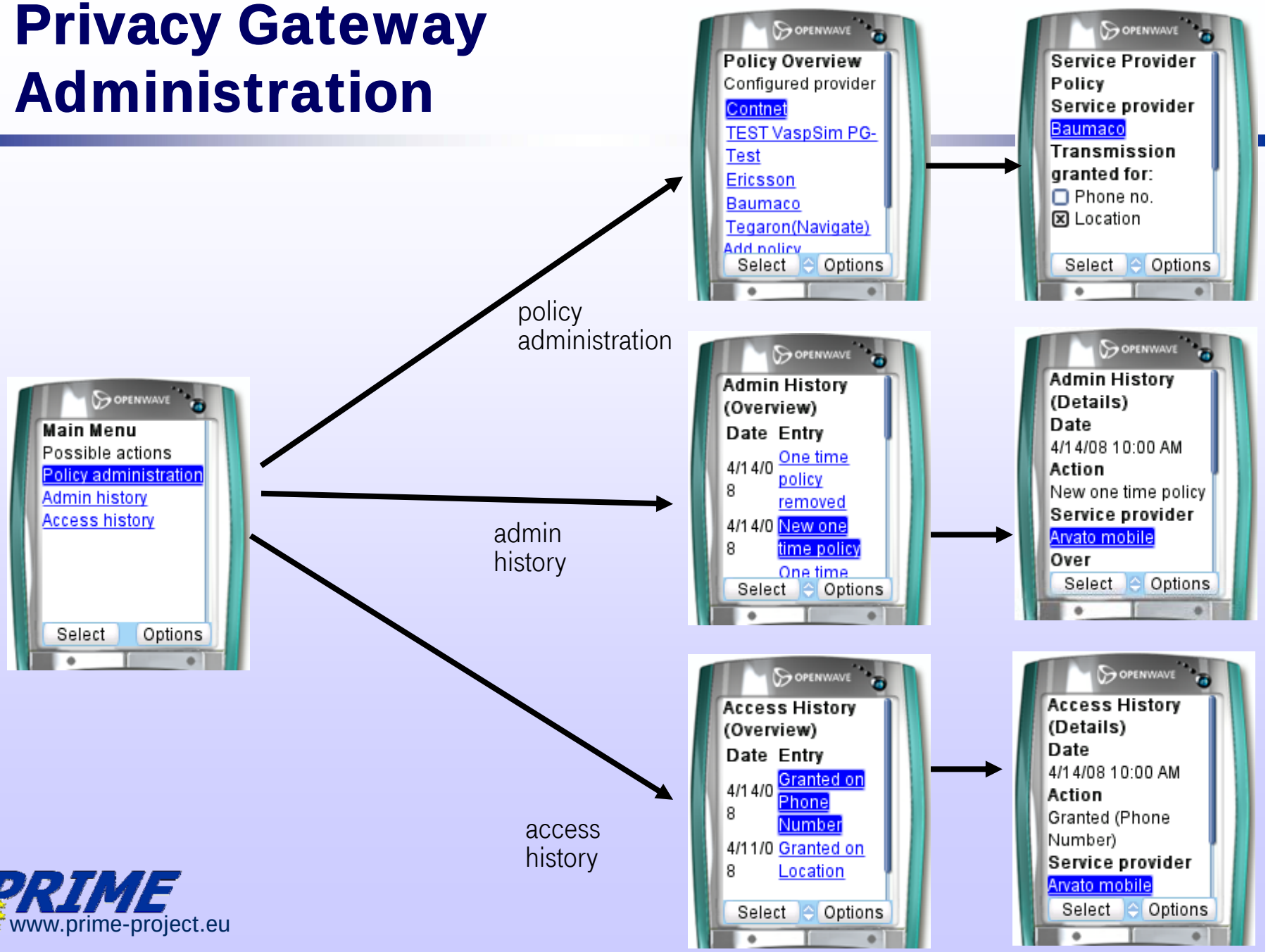
Product Transfer
Customer GUI



T-Zones / web'n'walk

Privacy Gateway Settings

Privacy Gateway Administration



PRIME
www.prime-project.eu

Agenda

- Privacy in a data intensive Information Society
- Identity Management
- Multilateral Security
- Enhancing Privacy via Intermediary Architectures and Choice
- Learnings for Development, Research, Standardisation
  - Philosophical Issues
  - Technical Design Principles for Multilateral Security
  - Challenges and Potential for Research and Standardisation
  - Challenges & Potential for Europe
- Conclusions & Outlook

Agenda

- Privacy in a data intensive Information Society
- Identity Management
- Multilateral Security
- Enhancing Privacy via Intermediary Architectures and Choice
- Learnings for Development, Research, Standardisation
  - Philosophical Issues
  - Technical Design Principles for Multilateral Security
  - Challenges and Potential for Research and Standardisation
  - Challenges & Potential for Europe
- Conclusions & Outlook

7 Ps for Privacy and PETs

- Phantasy
- Persistence
- Patience
- Perspiration
- Passion
- Personality
- Political Support

mobile business

Agenda

- Privacy in a data intensive Information Society
- Identity Management
- Multilateral Security
- Enhancing Privacy via Intermediary Architectures and Choice
- Learnings for Development, Research, Standardisation
  - Philosophical Issues
  - Technical Design Principles for Multilateral Security
  - Challenges and Potential for Research and Standardisation
  - Challenges & Potential for Europe
- Conclusions & Outlook

Technical Design Principles for Multilateral Security 1/2

Data Economy

- Avoidance of all data that is not really needed, e.g. protocols, that do the same service with less data (implicit adresses, limited broadcast, ...)

Careful allocation

- Avoidance of large data collections under responsibility of **one** entity, e.g. no HLR in mobile communication networks
- Reachability data in users' PDAs

User ability to configure and control

- Useful status information ("Where is my data, where will it go, after I click that button ?")
- Warning function of digital signatures

Technical Design Principles for Multilateral Security 2/2

Usability

- There is **nothing** like **the** right solution as there is nothing like **the** user.

Opportunities for individual negotiation

- **Negotiation** needs **choice**.

Discernable security

- **Sustainable** security **marketing** needs security **recognition.**
- **Recognition** needs **awareness** and **comprehension** of **advantages**.
- **Comprehension** of advantages needs better **criteria.**

Agenda

- Privacy in a data intensive Information Society
- Identity Management
- Multilateral Security
- Enhancing Privacy via Intermediary Architectures and Choice
- Learnings for Development, Research, Standardisation
  - Philosophical Issues
  - Technical Design Principles for Multilateral Security
  - Challenges and Potential for Research and Standardisation
  - Challenges & Potential for Europe
- Conclusions & Outlook

Challenges and Potential for Research and Standardisation 1/2

- Empowering users to …
  - better control (identity) data flows
    - User-controlled hardware (Trustable computing) for
      - Identity data
      - (Anonymous) Communications
    - Transparent policies
  - select trusted partners from a choice of offers
    - Identity intermediary networks
    - Service provider networks
  - deal with the trade-offs
    - Testbeds to
      - Experience tradeoffs
      - … and quickly "feel" the results of the respective decisions.

Challenges and Potential for Research and Standardisation 2/2

- User-friendly Identity Management
  - in business processes and applications
  - in new communities and networks
  - along the value chain (with appropriate incentives)
  - considering the views of the respective stakeholders (Multilateral Security)
  - considering separations of domains that had been natural "before".
- Overcome the "Me too"-Approach

  "Any data that is used for providing a service must be available to law enforcement, too!"

Agenda

- Privacy in a data intensive Information Society
- Identity Management
- Multilateral Security
- Enhancing Privacy via Intermediary Architectures and Choice
- Learnings for Development, Research, Standardisation
  - Philosophical Issues
  - Technical Design Principles for Multilateral Security
  - Challenges and Potential for Research and Standardisation
  - Challenges & Potential for Europe
- Conclusions & Outlook

Challenges & Potential for Europe

- Raising trustworthiness of embedded systems
- (Standardized) reference architectures to integrate fragmented details
- Minimisation and decentralisation of data
- User-Centricity
- Identity Management

- Raising trustworthiness of embedded systems
  - Addressing e.g. computerized/networked cars and household appliances
  - Combining experiences from safety and IT Security
  - Improving transparency
  - ...

- (Standardized) reference architectures to integrate fragmented approaches
  - Privacy enhancing technologies (PETs)
  - Identity management
  - Credentials
  - Information flow control
  - …

- Minimising and decentralising data
  - Respecting proportionality
  - Reducing temptation
  - Avoiding misuse
  - Raising transparency on data flows
  - ...

Challenges & Potential User-Centricity

- Empowering users to …
  - better control of (identity) data flows
    - User-controlled hardware (Trustable computing) for
      - Identity data
      - (Anonymous) Communications
    - Transparent policies
  - select trusted partners from a choice of offers
    - Identity intermediary networks
    - Service provider networks
  - deal with the trade-offs
    - Testbeds to
      - Experience tradeoffs
      - … and quickly "feel" the results of the respective decisions.

Challenges & Potential Identity Management

- Considering
  - the views of the respective stakeholders (Multilateral Security)
  - separations of domains that had been natural “before”
- Enabling users to manage their identities
- Frameworks and reference architectures
  - Along the value chain (with appropriate incentives)
  - For business processes and applications
  - For new communities and networks
- Globally standardized (e.g. in ISO/IEC JTC 1/SC 27/WG 5 “Identity Management and Privacy Technologies)

Related Standardisation

- ISO/IEC JTC 1/SC 27/WG 5: Identity Management & Privacy Technologies
  - ISO/IEC 24760 Framework on Identity Management
  - ISO/IEC 29100 Privacy Framework
  - ISO/IEC 29101 Privacy Architecture
- ISO/IEC JTC 1/SC 27/WG 3: IT Security Evaluation Criteria
- ITU-T SG 13 (NGN), SG 17 (Security)
- ETSI/HF Specialist Task Force STF265 on User Profile Management

Agenda

- Privacy in a data intensive Information Society
  - Mobility and Privacy
  - Mobile Business
  - Mobile Advertising
- Identity Management
- Multilateral Security
- Enhancing Privacy via Intermediary Architectures and Choice
- Learnings for Development, Research, Standardisation
- Conclusions & Outlook

mobile business

Conclusions & Outlook

- ICT and new services are coming ever closer to people, e.g. in **advertising** and **recommendations**.
- ➢ Privacy and Multilateral Security getting ever **more important** for trust
- **Challenges** and **potential** in
  - Privacy and Identity **infrastructures**
  - **Multilaterally secure tools**, that help users to manage their Privacy and Identity
- First elements of Identity Management and Privacy Technologies are being **standardized** globally (ISO/IEC JTC 1/SC 27/WG 5).
- Who wants **trust** needs to **overcome** the **"Me too"-Approach.**

Questions/Comments welcome

- Kai.Rannenberg@m-chair.net
- www.m-chair.net
- www.fidis.net
- www.prime-project.eu
- www.primelife.eu
- www.picos-project.eu

Literature

- [BlaBorOlk2003] G. W. Blarkom, John J. Borking, and J.G. Olk. Handbook of Privacy and Privacy-Enhancing Technologies - PISA Privacy Incorporating Software Agent. The Hague, 2003.
- FIDIS: Future of Identity in the Information Society; www.fidis.net
- Stefan Figge, Gregor Schrott, Jan Muntermann, Kai Rannenberg: EARNING M-ONEY - A Situation based Approach for Mobile Business Models; Proceedings of the 11th European Conference on Information Systems (ECIS) 2003; June 19-21, 2003, Naples, Italy
- German Constitutional Court: Decision on Online –Trojans and the basic right to confidentiality and integrity for IT systems; 2008-02-27; www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html; www.edri.org/edrigram/number6.4/germany-constitutional-searches
- [ICDPPC 2005] The 27th International Conference of Data Protection and Privacy Commissioners: “The protection of personal data and privacy in a globalised world: a universal right respecting diversities (The Montreux Declaration)”, 2005-09-14/16; Montreux, Switzerland; www.privacyconference2005.org/fileadmin/PDF/montreux_declaration_e.pdf
- ISO/IEC JTC 1/SC 27/WG 5: Identity Management and Privacy Technologies; www.jtc1sc27.din.de
- PICOS: Privacy and Identity Management for Community Services; www.picos-project.eu
- PRIME: Privacy and Identity Management for Europe; www.prime-project.eu
- PrimeLife: Privacy and Identity Management for Life; www.primelife.eu

mobile business

Literature

- Kai Rannenberg: Multilateral Security – A concept and examples for balanced security; Pp. 151-162 in: Proceedings of the 9th ACM New Security Paradigms Workshop 2000, September 19-21, 2000 Cork, Ireland; ACM Press; ISBN 1-58113-260-3
- Kai Rannenberg: Identity management in mobile cellular networks and related applications; Information Security TR; Vol. 9, No. 1; 2004; pp. 77 – 85; ISSN 1363-4127
- [Reagle1998] Joseph M. Reagle Jr., Boxed In: Why US Privacy Self Regulation Has Not Worked, Berkman Center for Internet & Society, Harvard Law School, 1998, http://cyber.law.harvard.edu/people/reagle/privacy-selfreg.html
- T-Mobile Chair for Mobile Business & Multilateral Security; www.m-chair.net
- [WaBr1890] Samuel D. Warren, Louis D. Brandeis: The Right to Privacy", Harvard Law Review; Vol. IV; December 15, 1890, No. 5; www.lawrence.edu/fac/boardmaw/Privacy_brand_warr2.html
- Jan Zibuschka, Lothar Fritsch, Mike Radmacher, Tobias Scherner, Kai Rannenberg: Enabling Privacy of Real-Life LBS: A Platform for Flexible Mobile Service Provisioning; in Proceedings of the 22nd IFIP TC-11 International Information Security Conference 2007; 14-16 May 2007, Sandton, South Africa; Springer IFIP Series
- Jan Zibuschka, Mike Radmacher, Tobias Scherner, Kai Rannenberg: Empowering LBS Users: Technical, Legal and Economic Aspects; in: Proceedings of the eChallenges conference 2007; The Hague, The Netherlands